ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE ENGINEERING AND TECHNOLOGY

AN INVESTIGATION ON RISK ANALYSIS METHODS TO BE USED FOR THE PREVENTION OF MAJOR INDUSTRIAL ACCIDENTS

M.Sc. THESIS

Asadulla KHALILOV

Department of Chemical Engineering

Chemical Engineering Programme

JULY 2015

ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE ENGINEERING AND TECHNOLOGY

AN INVESTIGATION ON RISK ANALYSIS METHODS TO BE USED FOR THE PREVENTION OF MAJOR INDUSTRIAL ACCIDENTS

M.Sc. THESIS

Asadulla KHALILOV

506131002

Department of Chemical Engineering

Chemical Engineering Programme

Thesis Advisor: Assist.Prof. Dr. Hikmet İSKENDER

JULY 2015

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

BÜYÜK ENDÜSTRİYEL KAZALARIN ÖNLENMESİ İÇİN KULLANILAN RİSK ANALİZ YÖNTEMLERİ ÜZERİNE BİR İNCELEME

YÜKSEK LİSANS TEZİ

Asadulla KHALILOV
506131002

Kimya Mühendisliği Anabilim Dalı

Kimya Mühendisliği Programı

Tez Danışmanı: Yrd.Doç.Dr.Hikmet İSKENDER

TEMMUZ 2015

Asadulla KHALILOV, an **M.Sc.** student of ITU **Graduate School of Science Engineering and Technology** 506131002, successfully defended the **thesis** entitled **'AN INVESTIGATION ON RISK ANALYSIS METHODS TO BE USED FOR THE PREVENTION OF MAJOR INDUSTRIAL ACCIDENTS'**, which he prepared after fulfilling the requirements specified in the associated legistations, before the jury whose signatures are below.

Thesis Advisor : **Assist.Prod.Dr Hikmet İSKENDER** **……..**
Istanbul Technical University

Jury Members : **Prof Dr Dursun Ali ŞAŞMAZ** **……..**
Istanbul Technical University

Prof Dr Ülker BEKER **……**

Date of Submission : 07 July 2015
Date of Defense : 07 July 2015

To my family,

FOREWORD

I would like to thank my supervisor Dr Hikmet ISKENDER for giving me valuable advice and support always when needed. And also I like to give special thanks to BOTAS Inc. employees for giving me an oppurtunity to share their knowledge and the best available information about BOTAS Inc.

July 2015

Asadulla KHALILOV

Chemical Engineering

TABLE OF CONTENTS

Page

ABBREVIATIONS

CHIP	**:** Chemicals Hazard Information and Packaging for Supply
CLP	**:** Classification, Labeling and Packaging of Substances and Mixtures
COMAH	**:** Control of Major Accident Hazards
ETA	**:** Event Tree Analysis
EPA	**:** Environmental Protection Agency
FMEA	**:** Failure Mode and Effect Analysis
FTA	**:** Fault Tree Analysis
MSDS	**:** Material Safety Data Sheet
HAZOP	**:** Hazard Operability Study
PrHA	**:** Process Hazard Analysis
P&ID	**:** Process and Instrumental Diagrams

LIST OF TABLES

Page

LIST OF FIGURES

Page

AN INVESTIGATION ON RISK ANALYSIS METHODS TO BE USED FOR THE PREVENTION OF MAJOR INDUSTRIAL ACCIDENTS

SUMMARY

Generally in the industry, there are a lot of industry's types within the hazard class. One of the most hazardous types of industry is the Chemical Industry. If we do not eliminate dangers and do not take necessary measurements, the major industrial accidents can be occur with the deaths, injuries and economic losses.
Major industrial accidents involving dangerous chemicals pose a significant threat to humans and the environment. However, the use of large amounts of dangerous chemicals is unavoidable in some industry sectors which are vital for a modern industrialised society. To minimise the associated risks, measures are necessary to prevent major accidents and to ensure appropriate preparedness and response should such accidents nevertheless happen.
One of the major industrial accident was happened in Italian town of Seveso in 1976. An explosion occured in a TCP (2,4,5 – trichlorophenol) reactor of the ICMESA chemical plant. After the explosion, a toxic cloud containing TCDD (2,3,7,8 – tetrachlorodibenzo – p –dioxin) was accidentally released into the atmosphere. This event became internationally known as the Seveso disaster. In Europe, the catastropic accident prompted the adoption of legistation on the prevention and control of such accidents. The so-called Seveso-Direcitve (Directive 82/50/EEC) and was adopted in 1982 by the Europian Union (EU). The Seveso Directive aims at the prevention of major accidents involving dangerous substances. However, as accidents may neverless occur, it also aims at he limiting the consequences of such accidents not only for human health but also for the environment. SEVESO was later amended in view of the lessons learned from later accidents such as Bhopal, Toulouse or Enschede resulting into Seveso-II (Directive 96/82/EC) in 1996. And also in 2003, Seveso II was revised proposal as Extended Seveso II (Directive 2003/105/EC). Application depends on inventory of dangerous substances, currently defined using CHIP(Chemicals Hazard Information and Packaging for Supply) regulations eg toxic, very toxic etc. But CHIP is on the way out and the CLP(Classification, Labelling and Packaking of Substances and Mixtures) Regulations are on the way in and without the new Seveso III Directive, Seveso/COMAH would cease to funtion. Lastly, in 2012 Seveso-III (Directive 2012/18/EEC) was adopted by EU and will come into force from 1st January 2016. The main approach stays the same : 3 part strategy : identification; control; & mitigation. Seveso III will have the same component parts: safety management of sites cabaple of producing major accident hazards, emergency planning, land use planning & inspection. It replaces the previous Seveso II directive.

The main areas of change in the Seveso III Directive are:

- Scope – how the system will move from CHIP classification to CLP – i.e. which substances are in/ out.
- Public info – more requirements than in Seveso II.

- Inspection - kept the current approach of hazard/risk based inspections.
- Correction system - there is currently no legal method for taking substances out of scope the Seveso III Directive i.e. substances which come into scope of the CLP classification but are considered not to have major accident potential. There is currently work going on in Europe to look at this but there is no easy solution as any change would require the Commission to put forward a proposal to amend the Directive.

The Directive contains general and specific obligations on both the competent authorities of the member states and industrialists. One of the issues covered by Seveso Directive is to perform Process Hazard Analysis (PHA) for the plants. Process Hazard Analysis is a set of organized systematic assessments of the potential hazards associated with an industrial process. There are varieties of methodologies that can be used to conduct a PHA and the most known methodology is the Hazard and Operability Study (HAZOP). A HAZOP is systematic approach to investigating each element of a process to identify all of the ways in which parameters can deviate from the indented design conditions and create hazards or operability problems. A HAZOP study typically involves using Piping and Instumental Diagrams (P&ID), or a plant model, as a guide for examining every section and component of aprocess.

The Seveso II entered into force in Turkey in 30th December 2013. In 1st January 2016, the Seveso II will dismantle and Seveso III will take place of Seveso II in Europe. The main purpose of this study that contirbutes to great industrial plants which are located in Turkey, to pass from Seveso II to III and exemplary the BOTAS (Petroleum Pipeline Corporation) Inc. plant was analyzed. The hazards and potential risks were determined in BOTAS, and potential scenarios were written for plant and the event of these scenarios, plant's impact on ecosystem and environment are determined by computer programme.

BÜYÜK ENDÜSTRİYEL KAZALARIN ÖNLENMESİ İÇİN KULLANILAN RİSK ANALİZ YÖNTEMLERİ ÜZERİNE BİR İNCELEME

ÖZET

Genel olarak endüstri içinde : bir çok tehlike sınıfına giren sanayi kolları vardır. Bu sanayi kollarının en tehlikesi 'Kimya Endüstrisidir'. Var olan bu tehlikeleri ortadan kaldırmaz ve gerekli tedbirleri almazsak, ölümler, yaralanmalar ve yüksek ekonomik kayıplarla ile sonuclanan büyük kazalar meydana gelmektedir.

Büyük Endüstriyel Kazalar tanımı ile, herhangi bir işletmede, kontrolsüz gelişmelerden kaynaklanan ve tesis içinde veya dışında insan sağlığı için anında veya sonrasında ciddi tehlikelere yol açabilen, bir veya birden fazla tehlikeli maddenin sebep olduğu büyük yayılımları, yangınları veya patlamaları ifade etmektedir.

Bu çalışmanın konusu olan Büyük Endüstriyel Kazalardan biri 10 temmuz 1976'da İtalyanın Lombardiya bölgesinin Seveso kasabasında küçük bir kimyasal üretim fabrikasında meydana gelmiştir. Triklorofenol (TCP) üretmek için diğer rakip şirketlere göre daha tehlikeli bir reaksiyon kullanılması ve reaktörün yeterince soğutulmadan bırakılmasına olanak sağlayan tehlikeli işletim uygulamaları bu önemli kazanın oluşma nedenleridir. Ekzotermik bir kimyasal reaksiyonun kontrolünün kaybedilmesi, patlama diskinde ve basınç tahliye sisteminde reaktörün içeriğinin atmosfere salınmasına yol açmıştır. Toksik ve korozif kimyasallardan oluşan, fenol, sodyum hidroksit ve 2,3,7,8-tetrachlorodibenzo-p-dioksin (TCDD – 'Seveso Dioksin') içeren bir gaz bulutu çevreye yayılmıştır. Bu zehirli gaz, bu güne kadar bilinen en zehirli gazlardan dioksindir. Kasabada kısa bir süre içinde hayvan ölümleri görülmeye başlanmış, patlamadan 5 gün geçtikten sonra da hastaneye başvurular başlamıştır. Yapılan kontroller sonunda kasabada geniş bir bölgenin tamamen kirlendiği anlaşılmış ve 100 kadar ev tamamne boşaltılmışdır.

Dioksin (TCDD) besin zincirine katılan ve etkileri uzun yıllar devam eden tehlike sınıfı yüksek bir kimyasal olduğu için o bölgede halen tarım faaliyeti yapılmamaktadır.

Seveso felaketinden sonra Avrupa ülkelerinde endüstriyel kazalara karşı mevcut önlemlerin yetersiz olduğu sonucuna varılarak bir dizi çalışma başlatıldı. O zamanki adıyla Avrupa Topluluğu Konseyi (EC), yapılan çalışmalar sonucunda tehlikeli maddelerle ilgili büyük endüstriyel kazaların kontrolü ve önlenmesi ile ilgili 'Seveso Yönergesi (Direktifi)'ni 24 Haziran 1982 tarihinde yayınladı.

Ancak SEVESO Direktifi sonrasında da 1984 Bhopal felaketi başta olmak üzere gerek dünyada gerek Avrupa'da devam eden Büyük Endüstriyel Kazalar sonrasında, bu direktifin etkinliğinin artırılması ve kapsamının genişletilmesi amacıyla 1996 yılında 96/82/EC SEVESO II Direktifi yayınlanmış, 2003 yılın da bir kez daha gözden geçirilerek 2003/105/EC 'Genişletilmiş Seveso II Direktifi' olarak revize edilmiştir. Son olarak da 2012/18/EEC sayılı SEVESO III Direktifi, 26 Haziran 2012 tarihinde AB Bakanlar Konseyi'nde kabul edilmiştir. Yeni direktif 1 Ocak 2016 tarihinde yürürlüğe girecektir. Direktifin ana hatları aşağıdakı gibidir :

- Direktif'te detaylı şekilde tanımlanan görevlerin yerine getirlmesi için bir yetkili otoritenin belirlenmesi
- Kazaların domino etkileri
- Arazi Kullanım Planlaması, çevre etkileri
- Risk Değerlendirme Metodolojisi ve Kaza Senaryoları, tatbikatlar
- Kamu Bilgilendirilmesi
- Büyük Endüstriyel Kazalar sırasında uygulanacak dahili ve harici Acil Durum Planlarının (ADP) hazırlanması, gözden geçirlimesi, test edilmesi ve revize edilmesi.
- Büyük endüstriyel kazaların araştırılması, raporlanması ve denetimi
- Kimyasalların sınıflandırılması, paketlenmesi ve etiketlenmesi

Direktif hem sanayiciler üzerindeki hem de üye devletlerin yetkili makamları üzerinde genel ve özel yükümlükleri içerir. İşletmeci, büyük kazaları ve büyük bir kazanın meydana gelmesi durumunda, bunların etkilerini çevre ve insanlara en az zarar vercek şekilde sınırlamak için gerekli tüm tedbirleri almakla yükümlüdür. Direktifin kapsadığı konulardan biride, tesis için Proses Tehlike Analizinin yapılmasıdır. Bir endüstriyel süreçle ilgili potansiyel tehlikelerin değerlendirlmesinin organize ve sistematik bir set oluşturarak yapılmasına 'Proses Tehlike Analizi' denilmektedir. Proses tehlike analizi gerçekleştirmek için çok çeşitli yöntemler olup, bunlardan en bilineni HAZOP'tur. Tehlike ve İşletilebilirlik Çalışması şeklinde bilinen HAZOP, özellikle kimsayal, ilaç ve petrokimya sektörlerinde en fazla kullanılan metoddur. HAZOP çalışması sonucunda eksik yada gerekli Proses Emniyet Bilgileri (Process Safety Information – PSI) ve ayrıca tüm proses tehlikeleri belirleniyor. PSI verileri normal operasyonlardan sapmaların sonuçlarını değerlendirmek için kullanılır. Sonuçlar değerlendirildikten sonra işletme (tesis) için risk derecendirilmesi yapılarak olasılıkların izin verilen seviyelere indirilmesi amacıyla güvenlik bariyerlerine ihtiyaç duyulup duyulmacağına karar verilir ve ayrıca sonuçlar bilgisayar program ile ayrıca değerlendirilir.
Seveso – II Direktifinin Türkiye mevzuatına uyumlaştıran 'Büyük Endüstryiyel Kazaların Önlenmesi ve Etkilerinin Azaltılması Hakkında Yönetmelik' Çevre ve Şehircilik Bakanlığı ve Çalışma ve Sosyal Güvenlik bakanlığınca oluşturulan bir komisyon ile hazırlanarak, 30 Aralık 2013 tarih ve 288867 Mükerrer sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.
Mevzuata göre Seveso Kapsamında yapılması gerekenler :

- Büyük Kaza Önleme Politika Belgesi (BKÖP)
- Güvenlik Raporu
- Kantitatif Risk Değerlendirmesinin Yapılması (QRA)
- Mümkün Olan En Yüksek Önlem Seviyesi
- Güvenlik Yönetim Sistemi Kurulması
- Dahili Acil Durum Planı
- Harici Acil Durum Planı
- Denetimler

Belirtildiği gibi Türkiye'de SEVESO II direktifi 30 Aralık 2013 yılında yürürlüğe girmiştir. 1 Ocak 2016 tarihinde SEVESO II AB'de yürürlükten kaldırılacak ve yerini SEVESO III alacak. Bu çalışmanın ana amacı Türkiyede bulunan önemli endüstriyel tesislerin SEVESO II den SEVESO III geçmesinde katkıda bulunmak, ve örnekleme için BOTAŞ (Boru Hatları ile Petrol Taşıma) A.Ş. tesisi incelenmiştir.

Yaşanmış büyük petrol yayılımları, yangınları ve patlamaları örnekler ile verilirken, dünya çapında geçerliliği olan yönetmelikler baz alınarak, yaşanmış tüm bu olayların bir daha yaşanmaması için ve olası risklerin önlenmesi için bu çalışma yapılmıştır. Tesisde bulunan eksikler belirlenmiş, kantitatif risk değerlendirmesine göre belirlenen kritik ve tehlikeli ekipmanlar ve olası risklere uygun senaryolar yazılmış ve bu senaryoların gerçekleşmesi durumunda tesisin görebileceği zararları ve ekosisteme olacak etkileri yazılım programı ile belirlenmiştir.
Elde edilen modellemeler aşağıdakı gibidir :

- Yayılım Modeli (Release)
- Atmosferik Dağılım Modeli
- Pool/Havuz Evaporasyon Modeli
- Termal Radyasyon / Yanma Modeli
- Patlama Modeli
- Kombine Modellemeler

1. INTRODUCTION

The development of process and design of chemical plant for the conversion of raw material into final products come under chemical enginnering. Process risk analysis is an important activity, which is to be performed at different life stages of process not only to meet the standarts/regulations but also for the improvement of the process and/or plant.

Incidents and accidents especially the well known catastrophic accidents in Flixborugh (UK) , Seveso (Italy) and Bhopal (India) have shown that effects of process/plant malfuntion may not only be hazardous to operators but also catastrophic to human life (including members of public), environment and/or capital. Therefore, removing process/plant malfunctions for reduction of risk and prevention of such accidents in future is of interest for community and company and an emerging subject of chemical engineering as well[1].

Several directives in the Euopean community, e.g. EC Directive of Major Accident Hazards [2] and Atex Directives 137 (1999/92/EC) and 100A (84/9/EC /3/ for safety and health protection of workers from explosive atmospheres, are based on safety/risk analysis techniques.

However, basic factors determining the magnitude of hazard (1-3) and risk(1-9) are:

1. inventory and properties of hazardous materials (volatility, toxicity, reactivity)
2. type of operation; process conditions
3. complexity of operations
4. design and operation relative to standards and codes
5. layout of equipment
6. plant layout (distance of equipment)
7. preventive and protective measures
8. plant site (distance to population centers, vulnerability of the surrounding)
9. effectiveness of plant management (operator training, production vs.risk)

To come from hazardous process (idea) to safe operation (safe operation means the risk is small enough to be tolerated by community and company) safety/risk analysis work is relevant during process development, plant design and plant operation as well. In addition to safety/risk analysis techniques, inherent safety design practices are also used in order to improve the process, technology and management[3].

2. RISK TERMINOLOGY

2.1 What is the Hazard ?

Hazard is a physical situation with a potential for human injury,damage to property, damage to the environment or some combination of these or we can say a hazard is acombination of a hazardous material, an operating environment, and certain unplanned events that could results in a accident. The degree of hazard depends on inventory and properties of hazardous materials (volalitility, toxicity, reactivity) type of operation and process conditions[4].

2.2 What is the Risk ?

Risk describes the frequnecy and magnitude of damage e.g. financial risk may be expressed as a product of frequency and damage costs (Risk = frequency x consequency).

2.3 What is the Risk Calculation?

Risk calculation has to consider the objective, which may be focused on an individual (operator or public at fence) , society or company. Invidual risk may be raleted to financial, injury or death. Societal risk may include number of injuries or deaths, contimination of the environment and/or property damage. Company interests may be related to economical aspects and/or loss of production/market.

2.4 Inherent Safety Measure

Inherent safety measures may be classified in material/chemical, process or construction effects. Reducing inventories of hazardous materials, or – if possible – replacing them by less hazardous chemicals is the preferred inherent safety measure. Next, a less hazardous process, reduction of process parameters (temperature, pressure) will increase inherent safety as well. A simplified construciton and design related to maximum pressure possible, e.g as s result of run away reactions, characterize the third class[5].

2.5 Hazard Assessment

Hazard assessment ends with evaulating various amounts of emissions of hazardous (flammable, toxic) chemicals.

2.6 Safety/Risk Analysis

Safety/risk analysis is a qualitative/quantitative estimate of risk based on damage and frequency analysis of relevant harmful events.

2.7 Risk Assessment

Risk assessmnet underlines the point that the study ends with the assessment of resulting consequences in terms of fatalities and/or damage loss.

2.8 Frequency

Frequency is the number that event (failure or damage) occurs per time.

2.9 Probability

Probability describes the likelihood that event will succeed or not. The probability number is between 1 and 0 and has no unit.

2.10 Failure

Failure is when a system is incapable of carrying out its duty. Systems can fail either to a dangereous condition or to a safe condition. Revealed failure will be detected at the time of failure exist. Unrevealed failure will remain undetected until to the time of routinely proof test.

3. RISK MANAGEMENT

The sound management of chemicals throughout their life-cycle is an essential national activity in order to minimise risk, and/or prevent the occurrence of adverse impacts. The function of risk management is to decide whether a level of risk is acceptable, and if not, to translate the information into policies and actions designed to, for example, control exposure, to reduce risk through national legislative action, or to reduce risk in a variety of other ways[6].

Human health and environmental risks can occur at any, or all of the stages of a commercial chemical life-cycle, which may consist of:

- extracting and refining industries;
- chemical manufacturers and processors;
- chemical formulators;
- individual customers; and
- chemical disposers.

3.1 What is Risk Management ?

The risks associated with a potential for harm due to exposure to chemicals have to be identified, assessed and managed appropriately. The distinction between assessment and management of risks is a key issue. Much has been written on the purpose and implementation of the risk assessment procedure, which is designed to evaluate, usually quantitatively, the nature and magnitude of a potential risk. But on its own, risk assessment has limited value[6].

Risk management on the other hand, is the decision-making process to accept a known or assessed risk and/or the implementation of actions to reduce the consequences or probabilities of such an occurrence. Various definitions of risk management have been developed by national organisations and institutions. According to the United States Presidential/Congressional Commission on Risk Assessment and Risk Management (1997), risk management '*is the process of identifying, evaluating, selecting, and implementing actions to reduce risk to human health and to ecosystems. The goal of risk management is scientifically sound, cost-*

effective, integrated actions that reduce or prevent risks, while taking into account social, cultural, ethical, political, and legal considerations.'

When developing risk management decision-making strategies, two complementary approaches are considered, usually in sequence:

- effects – oriented policies : effects on human health ant the environment; and
- source – oriented policies: prevention of effects by controlling releases.

The effects of a chemical on health and the environment via an exposure pathway, for example, represents the first important parameter. Then suitable exposure standards can be developed. These standards are then translated into a source-related policy to control the releases of the chemical to ensure that exposure standards are not exceeded. Risk management therefore considers both policies.

In more general terms, risk management decision-making should embody a systematic, and structured approach to chemical risks, that allows the parties involved to:

- identify risks/problems that need to eliminated or reduced – to evaluate;
- identify ways in which these risks can be eliminated or,'managed' – to control; and;
- decide upon the most appropriate strategy to achieve reduction of risk – to implement and monitor.

The risk management process can also be described as comprising a six-step process, ranging from identification of the problem to evaluation of control actions. The process is an iterative one and not a linear sequence of actions. The six steps have been recognised as an important cyclical process to follow so that governments can make informed decisions on priority chemicals. Conducting a situation analysis/needs assessment.

1. Developing the risk reduciton goal,sub-goals and indicators
2. Identifying and evaluating possible risk reduction options
3. Obtaining commitment from decisin-makers and taking action
4. Evaluating Impact

As health and environmental problems caused by chemicals can sometimes be extremely complex to solve, experience from many countries shows that a well-organised risk management decision-making process, such as is outlined here, can

assist in problem identification and taking appropriate action. This complexity is caused by a combination of factors:

- The large of chemical subsances is commerce and substances of natural origin with which human beings come into contact, along with pollutants, contaminants in food, commercial and househol products;
- Limited aviability of information concerning chemical use; many countries have insufficient data on the import, manufacture, trade, storage, transport, use and disposal of chemicals and chemical products;
- A high level of uncertainty concerning the precise hazardous nature and impact of chemicals, by themselves or in combination with order substances, on human health and the environment; and
- Divergent views amongst stakeholders, including public authorities, industry, consumers, trade unions, environmental groups, etc. with regard to the seriousness of the risks presented by chemicals , and on the appropriate responses[6].

4. RISK ASSESSMENT

Risk assesssment and risk analysis of technical systems can be defined as a set of systematic methods to identify hazards, quantity risks and determining of components, safety measures and/or human interventions for plant safety. Ideally risk analysis should done by bringing together experts with different backgrounds which are chemicals, human errors and process equipments[7].

4.1 Risk Assessment Steps

The scheme for qualitative and quantitative assessments:

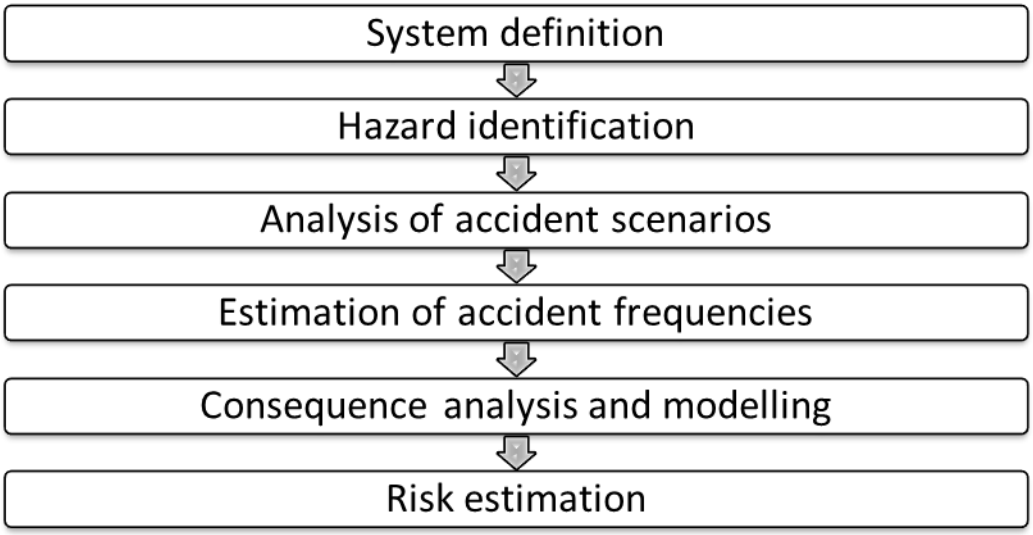


Figure 4.1 : Risk assesment steps.

At all steps, above table, risk reducing measures need to be considered.

4.2 Process Hazard Analysis

Prosess hazard analysis (PHA) is a semi-quantitative analysis that is performed to:

1. Identify all potential hazards and accidental events that may lead to an accident.
2. Rank the identified accidental events according to their severity.
3. Identify required hazard controls and follow up actions.

Several variants of PHA are used, and sometimes under different names like rapid risk ranking and hazard identification (HAZID)[8].

PHA can be used for :

- As an initial risk study in early stage of a project (e.g., of a new plant). Accicents are mainly caused by release of energy. The PHA identifies where energy may be released and which accidental events that may occur, and gives a rough estimate of the severity of each accidental event.The PHA results are used to (i) compare main concepts, to (ii) focus on important risk issues, and as (iii) input to more detailed risk anlyses.
- As an initial step of a detailed risk anlysis of a system concept or an existing system. Th purpose of the PHA is then to identify those accidental events that should be subject to a further, and more detailed risk analysis.
- As a complete risk analysis of a rather simple system. Whether or not a PHA will be a sufficient analysis depends both on the complexity of the system and the objectives of the analysis.

The PHA also shall consider about hazardous components, safety related interfaces between various system elements, environmental constraints including operating environments,operating, test maintanence, built-in-tests, diagnostics and emergency procedures,safety related equipments, safeguards, and possible alternate approaches.

Mainly, the PHA procedure is consist of four step.

1) PHA prerequisties is started with establish of PHA team and then system boundaries, process flow diagrams, block diagrams, use and storage of energy and hazardous materials in the sytem are defined and described. Risk information from previous and similar systems are also collected. A typical PHA tema may consist of a team leader, a secretary who will report the results and team members (2-6 persons) who can provide necessry knowledge and experience on the system being analyzed[8].

   As part of the system familiarization it is important to consider :

   - What is the system dependent upon ?
   - What activities are performed by the system ?
   - What services does the system provide ?

2) Hazard identification – All hazards and possible accidental events must be identified. It is important to consider all parts of the system, operational modes, maintanence operations, safety systems, and so on. All findings shall be recorded. No hazards are too insignificant to be recorded. Common soureces of hazards can be calssified as :
    - Sources and propagation paths of stored energy in electrcalical, chemical or mechanical form
    - Mechanical moving parts
    - Material or system incompalities
    - Nuclear and electromagnetic radiation
    - Collisions and subsequent problems of survival and escape
    - Fire and explosion
    - Toxic and corrosive liquids and gases escaping from containers or being generated as a result of other incidents
    - Biological hazards, including bacterial growth in such places as fuel tanks
    - Human error in operating, handling or moving near equipment of the system
    - Software error that can be cuse accidents
3) Frequency and consequence estimation – The risk related to an accidental event is function of the frequency of the event and the severity of its potential consequences. To determine the risk, we have to estimate the frequency and the severity of each accidental event. An accidental event may lead to wide range of consequences, ranging from negligible to catastrophic. A fire may, for example, be extenguished very fast and give minor consequneces, or lead to a disaster. In some applications the severity of an average consequence of an accidental event is assesed[8].

    Severity classes – the severity of an event may be classified into rather broad classes. An example of such a classificaiton is shown in Figure 4.2 and also frequnecy classification is shown in Figure 4.3.

.

Rank	Severity class	Description
4	Catastrophic	Failure results in major injury or death of personnel.
3	Critical	Failure results in minor injury to personnel, personnel exposure to harmful chemicals or radiation, or fire or a release of chemical to the environment.
2	Major	Failure results in a low level of exposure to personnel, or activates facility alarm system.
1	Minor	Failure results in minor system damage but does not cause injury to personnel, allow any kind of exposure to operational or service personnel or allow any release of chemicals into the environment.

Figure 4.2 : The severity classes.

1	Very unlikely	Once per 1000 years or more seldom
2	Remote	Once per 100 years
3	Occasional	Once per 10 years
4	Probable	Once per year
5	Frequent	Once per month or more often

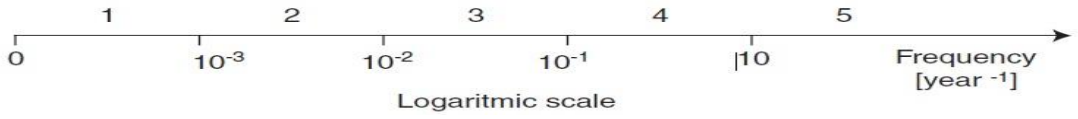


Figure 4.3 : The frequency classes.

4) Risk ranking and follow-up actions - The risk is established as a combination of a given event/consequence and a severity of the same event/consequence. This will enable a ranking of the events/consequences in a risk matrix as illustrated below :

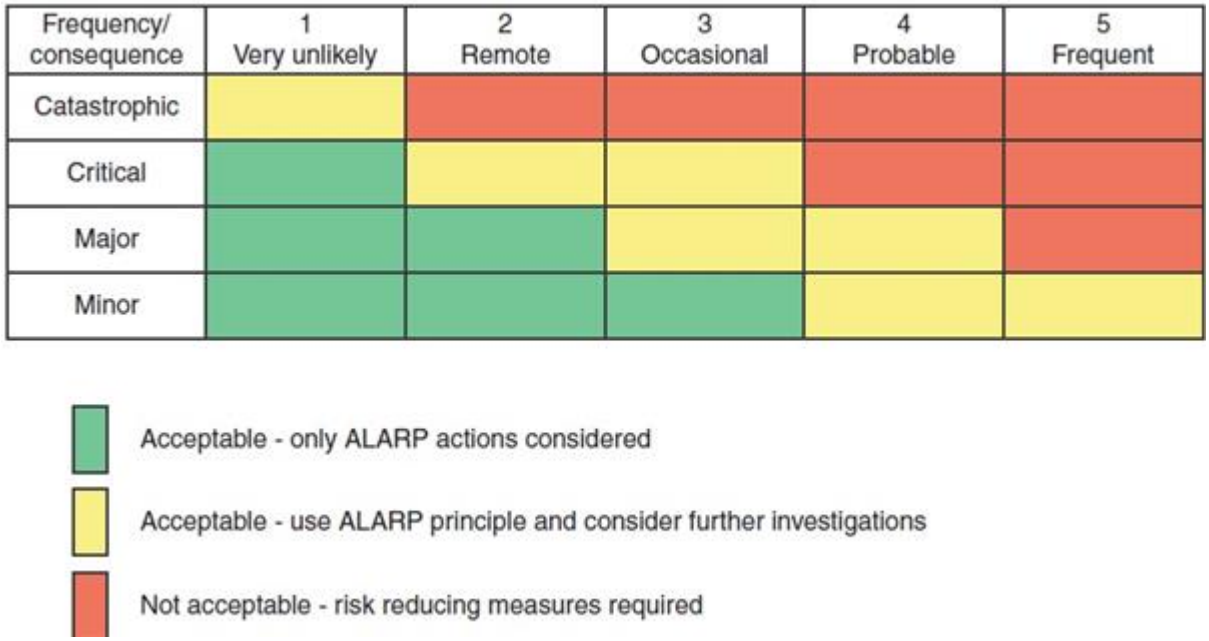


Figure 4.4 : Risk ranking and follow-up actions.

5. METHODS FOR HAZARD IDENTIFICATION

The selection of a PHA (Process Hazard Analysis) method depends on many factors including the size and complexity of the process and existing knowledge of the process[9].

One or more of the following methodologies as appropriate are used to determine and evaluate the hazards of the process being analyzed :

- What If
- Checklist
- What – If/Checklist
- Hazard and Operability Study (HAZOP)
- Failure Mode and Effects Analysis (FMEA)
- Fault Tree Analysis
- An appropriate equivalent

5.1 What –If Analysis

The purpose of a what-if analysis is to identify hazards, hazardous situations, or specific accident events that could produce an undesirable consequence. What-if analysis involves the examination of possible deviations from the design, construction, modification, or operating intent of a process. It can be used to examine virtually any aspect of facility design or operation. Because it is so flexible, it can be performed at any stage in the life of a process using whatever process information and knowledge is available[9].

5.1.1 Description of the method

The what-if analysis is a creative, brainstorming examination of a process or operation conducted by a group of experienced individuals able to ask questions or voice concerns about undesired events. It is not as inherently structured as some other methods, such as the hazard and operability (HAZOP) study or a failure mode and effects analysis (FMEA). Rather, it requires the analysts to adapt the basic concept to the specific application.

The what-if analysis encourages a PrHA team to think of questions that begin with "What-if." Through this questioning process, an experienced group of individuals identify possible accident events, their consequences, and existing safety levels, then suggest alternatives for risk reduction. The potential accidents identified are neither ranked nor given quantitative implications.

The what-if analysis method may simply generate a list of questions and answers about the process. However, it usually results in a tabular listing of hazardous situations, their consequences, safety levels, and possible options for risk reduction.

5.1.2 Analysis procedure

The information needed for a what-if analysis includes process descriptions, operating parameters, drawings, and operating procedures. All information must be available to the PrHA team, if possible, in advance of the team meetings. For analysis of an existing plant, the PrHA team may want to interview personnel responsible for operations, maintenance, utilities, or other services, if they are not on the PrHA team. In addition, if the analysis is performed offsite, the PrHA team should walk through the facility to better understand its layout, construction, and operation. Thus, visits and interviews should be scheduled before the analysis begins. Finally, some preliminary what-if questions should be prepared to "seed" the team meetings. If the analysis is an update of a previous PrHA, then questions listed in previous reports can be used. For a new process or a first-time application, preliminary questions should be developed by team members before the meetings, although additional questions formulated during the meetings are essential. The cause-and-effect thought process used in other types of analyses described in this section, such as HAZOP studies and FMEAs, can help formulate questions.

5.1.3 Limitations of the method

The what-if analysis is a powerful PrHA method if the analysis team is experienced and well organized. Otherwise, because it is a relatively unstructured approach, the results are likely to be incomplete[9][10].

5.2 Checklist Analysis

The checklist analysis method is versatile, easy to use and can be applied at any stage in the life of a process. It is primarily used to indicate compliance with standards and

practices. It is also a cost-effective way to identify common and customarily recognized hazards. Checklists also provide a common basis for management review of assessments. Many organizations use standard checklists to control the development of a process or an entire project from initial design through decommissioning. The completed checklist must be approved by all relevant staff members and managers before a project can move from one stage to the next.

5.2.1 Description of the method

A checklist analysis uses a written list of items or procedures to verify the status of a system. Checklists may vary widely in level of detail, depending on the process being analyzed. A traditional checklist analysis uses a list of specific items to identify known types of hazards, design deficiencies, and potential accident scenarios associated with common process equipment and operations. The method can be used to evaluate materials, equipment, or procedures. Checklists are most often used to evaluate a specific design with which a company or industry has a significant amount of experience, but they can also be used at earlier stages of development for entirely new processes to identify and eliminate hazards that have been recognized through operation and evaluation of similar systems. To be most useful, checklists should be tailored specifically for an individual facility, process, or product.

5.2.2 Analysis procedure

Performing a checklist analysis requires access to engineering design procedures and operating practices manuals and must be performed by a team with appropriate expertise. An experienced manager or staff engineer should review the results and direct follow-up actions.

A checklist is developed so that aspects of process design or operation that do not comply with standard industrial practices are discovered through responses to the questions in the list. A detailed checklist can be as extensive as necessary to satisfy the specific situation, but it should be applied conscientiously in order to identify problems that require further attention. Detailed checklists for particular processes should be augmented by generic checklists to help assure thoroughness. Generic checklists are often combined with other methods to evaluate hazardous situations. Checklists are limited by their authors' experience. They should be developed by individuals who have extensive experience with the processes they are analyzing.

Frequently, checklists are created simply by organizing information from current relevant codes, standards, and regulations. Checklists should be viewed as living documents and should be reviewed regularly and updated as required.

5.2.3 Limitations of method

When derived from handbooks or similar sources, many entries in a checklist may not be applicable to the process being studied. In other cases, process hazards may be so unusual they are not in standard checklists. Thus, it may be difficult to assure that all hazards have been analyzed. Also, checklists may indicate that hazards exist, but not what accident scenarios are associated with them[11].

5.3 What –If/Checklist Analysis

The purpose of a what-if/checklist anlysis is to identify hazards, consider the types of accidents that can occur in a process or activity, evaluate in a qualitative manner the consequences of these accidents, and determine whether the safety levels against these potential accident scenarios appear adequate.

5.3.1 Description of the method

The what-if/checklist analysis method combines the creative, brainstorming features of the what-if analysis with the systematic features of the checklist analysis. The PrHA team uses the what-if analysis method to brainstorm the types of accidents that can occur within a process. Then the team uses one or more checklists to help fill in any gaps. Finally, the team members suggest ways for reducing the risk of operating the process. The what-if analysis encourages the PrHA team to consider potential accident events and consequences that are beyond the experience of the authors of a good checklist and, thus, are not covered on the checklist. Conversely, the checklist lends a systematic nature to the what-if analysis.

Normally, a what-if/checklist analysis is used to examine the potential consequences of accident scenarios at a more general level than some of the more detailed PrHA methods. It can be used for any type of process at virtually any stage in its life cycle. However, this method is generally used to analyze the more common hazards that exist in a process.

5.3.2 Analysis procedure

For a what-if/checklist analysis, the PrHA team leader assembles a qualified team and, if the process is large, divides it into functions, physical areas, or tasks to provide some order to the review. For the checklist portion of the analysis, the PrHA team leader obtains or develops an appropriate checklist for the team to use. This list need not be as detailed as those used for a standard checklist analysis. Rather than focusing on a specific list of design or operating features, the checklist used here should focus on general hazardous characteristics of the process. In what-if analysis section, the PrHA team uses to develop questions about potential accident scenarios. After the team members have identified all of the questions in a particular area or step of the process, they apply the previously-obtained or prepared checklist. The team considers each checklist item to determine whether any other potential accident scenarios exist. If so, these scenarios are added to the what-if list and evaluated in the same way. The checklist is reviewed for each area or step in the process. After developing questions involving potential accident scenarios, the PrHA team considers each one; qualitatively determines the possible effects of the potential accident; and lists existing safety levels to prevent, mitigate, or contain the effects of the accident. The team then evaluates the significance of each accident and determines whether a safety improvement should be recommended. This process is repeated for each area or step of the process or activity. The evaluation may be performed by specific team members outside the team meeting but must be subsequently reviewed by the team.

5.3.3 Limitations of the method

Combining the what-if and checklist analysis methods emphasizes their main positive features (i.e., the creativity of what-if analysis and the experience-based thoroughness of a checklist analysis) while at the same time compensating for their shortcomings when used separately. For example, a traditional checklist is, by definition, based on the process experience the author accumulates from various sources. The checklist is likely to provide incomplete insights into the design, procedural, and operating features necessary for a safe process. The what-if part of the analysis uses a team's creativity and experience to brainstorm potential accident scenarios. However, because the what-if analysis method is usually not as detailed,

systematic, or thorough as some of the more regimented approaches (e.g., HAZOP study, FMEA), use of a checklist permits the PrHA team to fill in any gaps in their thought process[10][11].

5.4 Hazard and Operability Study (HAZOP)

The HAZOP study was developed to identify hazards in process plants and to identify operability problems that, although not hazardous, could compromise a plant's productivity. The basic concept behind HAZOP studies is that processes work well when operating under design conditions. When deviations from the process design conditions occur, operability problems and accidents can occur. The HAZOP study method uses guide words to assist the analysis team in considering the causes and consequences of deviations. These guide words are applied at specific points or sections in a process and are combined with specific process parameters to identify potential deviations from intended operation.

5.4.1 Description of the method

A HAZOP study requires considerable knowledge of the process, its instrumentation, and its operation. This information is usually provided by expert team members. The team should include individuals with a variety of experience, including design, engineering, operations, and maintenance[12].

The primary advantages of a HAZOP study are creativity and new ideas. Creativity is the result of interactions among team members with diverse backgrounds. Such interactions often generate new ideas. The success of a HAZOP study depends on the freedom of members to freely express their views. Combining this approach with a systematic protocol for examining hazards promotes thoroughness and accuracy.

5.4.2 Analysis procedure

A HAZOP study has three steps: (1) defining the process, (2) performing the study, and (3) documenting the results. Defining the process and documenting the results can be performed by a single person. The study itself must be performed by a team.

DEFINING THE PROCESS TO BE STUDIED. This step identifies the specific vessels, equipment, and instrumentation to be included in the HAZOP study and the conditions under which they are analyzed. Defining the problem involves defining the boundaries of the analysis and establishing an appropriate level of resolution for

the study. For most HAZOP studies, the causes of deviations are identified at the component level.

PERFORMING THE STUDY. A HAZOP study focuses on specific points of a process called "study nodes," process sections, or operating steps. Depending on the experience of the study leader, the portion of a process included in a single study node can vary. In the most conservative studies, every line and vessel are considered separately. If the HAZOP study leader is experienced, he or she may elect to combine two or more lines into a single study node. If too much of a process is included in a single study node, deviations may be missed. If too little of a process is included, the study can become tedious. In addition, root causes of deviations and their potential consequences can become separated. Too many study nodes is common for novice HAZOP study leaders. On the positive side, a study with too many nodes is less likely to miss scenarios than one with too few nodes[12].

DOCUMENTING THE RESULTS. The documentation of a HAZOP study is a systematic and consistent tabulation of the effects of process deviations. The study generates narratives about the normal operating conditions and analysis boundary conditions for each equipment item. In addition, it provides a list of potential actions that should be evaluated.

5.4.3 Limitations of the hazard and operability study

The primary limitation of a HAZOP study is the length of time required to perform it. Because the study is designed to provide a complete analysis, study sessions can be intensive and tiring. HAZOP studies typically do not look at occupational hazards (e.g., electrical equipment, rotating equipment, hot surfaces) or chronic hazards (e.g., chronic chemical exposure, noise, heat stress).

5.5 Failure Mode and Operability Analysis

5.5.1 Description of the method

A FMEA is used to examine each potential failure mode of a process to determine the effects of the failure on the system. A failure mode is the symptom, condition, or fashion in which hardware fails. It may be identified as a loss of function, a premature function (function without demand), an out-of-tolerance condition, or a

physical characteristic, such as a leak, observed during inspection. The effect of a failure mode is determined by the system's response to the failure[13].

5.5.2 Analysis procedure

A FMEA has three steps: (1) defining the process, (2) performing the analysis, and (3) documenting the results. Defining the process for study and documenting the results can be performed by a single person. The analysis itself must be performed by a team[13].

5.5.3 Defining the process

This step identifies the specific vessels, equipment, and instrumentation to be included in the FMEA and the conditions under which they are analyzed. Defining the problem involves establishing an appropriate level of resolution for the study and defining the boundary conditions for the analysis.

The required level of resolution determines the extent of detail needed in a FMEA. The choices for the level of resolution range from the subcomponent level to the system level. To satisfy PSM Rule requirements, most FMEAs should be performed at the major component level. This level provides the best trade-off between the time necessary to perform the analysis and the usefulness of the information gained from it.

Defining the analysis boundary conditions requires the following.

- Identifying the system or process to be analyzed.
- Establishing the physical boundaries of the systme or process.
- Establishing the analytical boundaries of the system or process.
- Documenting the internal and interface functions.
- Documenting the expected performance of the system, process, or equipment item; the system or process restraints; and the failure definitions of the equipment items, the process, or the system.
- Collecting up-to-date information identifying the process equipment and its functional relationship to the system

Functional narratives about the system or process should include descriptions of the expected behavior of the system or process and the equipment components for each operational mode. Narratives should describe the operational profiles of the components and the functions and outputs of each.

PERFORMING THE ANALYSIS. The FMEA should be performed in a deliberate, systematic manner to reduce the possibility of omissions and to enhance completeness. All failure modes for one component should be addressed before proceeding to the next component. A tabular format is recommended for recording results. A FMEA worksheet is produced by beginning at a system boundary on a reference drawing and systematically evaluating the components in the order in which they appear in the process flow path.

Failure Mode. The PrHA team should list all of the equipment item and interface failure modes. Given the equipment's normal operating condition, the team should consider all conceivable malfunctions.

Cause(s). If desired, the root causes of the failure mode should be identified. Identification of root causes provides information helpful for ranking hazards.

Operational Mode. If the equipment being analyzed is subject to different modes of operation, each operational mode should be identified and analyzed separately.

Effects. For each identified failure mode, the PrHA team should describe the anticipated effects of the failure on the overall system or process. The key to performing a consistent FMEA is to assure that all equipment failures are analyzed using a common basis. Typically, analysts evaluate effects on a worst-case basis, assuming that existing safety levels do not work. However, more optimistic assumptions may be satisfactory as long as all equipment failure modes are analyzed on the same basis.

Failure Detection Method. The means of failure detection should be identified, such as visual or warning devices, automatic sensing devices, sensing instrumentation, or other indicators. The main purpose of identifying failure detection methods is to determine whether the failure mode is "hidden," i.e., not detectable for some period of time. If there is no means to detect failure, "none" should be entered into the worksheet.

Compensating Provisions. For each identified failure mode, the PrHA team should describe any design provisions, safety or relief devices, or operator actions that can reduce the likelihood of a specific failure or mitigate the consequences.

Severity Class. The severity of the worst consequence should be specified as follows.

Category I - Catastrophic - May cause death or loss of system or process.

Category II - Critical - May cause severe injury, major property damage, or major system damage.

Category III - Marginal - May cause minor injury, minor property damage, or minor system damage.

Category IV - Minor - Is not serious enough to cause injury, propertydamage, or system damage, but may result in unscheduled maintenance or repair.

Remarks/Actions. For each identified failure mode, the PrHA team should suggest actions for reducing its likelihood or mitigating its effects. The actions suggested for a particular piece of equipment may focus on the causes or effects of specific failure modes or may apply to all of the failure modes collectively.

If the team discovers that a single item failure is not detectable, the FMEA should be extended to determine if the effects of a second failure in combination with the first could have catastrophic consequences. When a safety, redundant, or back-up component is evaluated, the analysis should consider the conditions that generated the need for the component.

DOCUMENTING THE RESULTS. A FMEA generates a qualitative, systematic reference list of equipment, failure modes, and effects. For each equipment item, the failure modes for that item and, if desired, the root causes for that failure mode are identified. For each failure mode, a worst-case estimate of the consequences is identified. This worst-case estimate assumes the failure of all protection against both the failure itself and the undesired consequences of the failure. The method by which the failure is detected is specified along with any compensating provisions. Finally, any suggestions for improving safety are listed in the table.

Limitaitons of Failure Mode and Effects Analysis

Human operator errors are not usually examined in a FMEA, but the effects of human error are indicated by an equipment failure mode. FMEAs rarely investigate damage or injury that could arise if the system or process operated successfully. Because FMEAs focus on single event failures, they are not efficient for identifying an exhaustive list of combinations of equipment failures that lead to accidents[14].

6. QUANTITAITVE RISK ANALYSIS TECHNIQUES

- Fault Tree Analysis
- Markov Processes
- Event Tree Analysis
- Monte Carlo Simulation

The most common way to model accident sequences is the event tree approach. This is particularly useful if the plant upset or equipment failure can result in different consequences from a risk stand point. If only one consequence needs to be analysed, all our quantitative methods can be applied.

If the probability of failure on demand of a safety system has to be calculated, the fault tree technique, or the Markov Processes or the Monte Carlo simulation can be used. If applied properly, all three methodologies will generate the same results, taking into account the constraints of each methodology and a proper comparison of the results generated with the different approaches.

6.1 Fault – Tree Analysis

6.1.1 Description

The fault tree technique can be described as an analytical technique, whereby an undesired state of the system is specified, and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur.

Fault tree analysis is a deductive failure analysis which focuses on one particular undesired event and which provides a method for determining causes of this event. The undesired event constitutes the top event in a fault tree diagram constructed for the system, and generally consists of a complete, or catastrophic, failure of the system under consideration. Careful formulation of the top event is important to the success of the analysis. The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event. The faults can be events that are associated with

component hardware failures, human errors, or any other pertinent event which can contribute to the top event[15].

It is important to understand that a fault tree is not a model of all possible system failures or all possible causes of system failure. A fault tree is tailored to its top event, which corresponds to some particular system failure mode, and the fault tree thus includes only those faults that contribute to this top event. It is also important to point out that a fault tree is not in itself a quantitative model. It is a qualitative model that can be evaluated quantitatively. The qualitative results generated with a fault tree are the minimal cut-sets and the qualitative insights which can be derived by evaluating the cut-sets[15].

A minimal cut-set is defined as a smallest combination of basic events that, if they all occur, will cause the top event to occur (for instance failure of a safety device). One speaks of a first-order minimal cut-set in case a single basic event causes the top event to occur. A second-order minimal cut-set is a combination of two single failures that, if they both occur, will cause the top event to occur.

A fault tree is a complex of entities known as ”gates” which serve to permit or inhibit the passage of a fault logic up the troth gates show the relationships of events needed for the occurrence of a ”higher” event. The ”higher” event is the ”output” of the gate ; the ”lower” events are the ”inputs” to the gate. The gate symbol denotes the type of relation of the input events required for the output event to occur. The lowest level events are called primary or basic events. Basic or primary events are singular events for which a probability of occurrence can be determined or estimated. These basic events can be associated with component hardware failure, human errors, maintenance or test unavailabilities or any other pertinent event that can contribute to the top event[16].

6.1.2 Qualitative analysis and quantitative analysis of fault tree method

To perform a fault tree analysis a number tasks have to be performed. In chronological order these tasks are :

Qualitative analysis:

- System familiarization.

  Before a fault tree can be constructed, one has to know in detail how the system operates and which failure modes have to be taken into account.
- Definiton of the top event and construction of the fault tree.

- Determination of the minimal cut sets.

Quantitative analysis:

- Collecting all relevant failure, repair,test and maintenance data.
- Quantification of the minimal cut-sets.
- Evaluation of the results.

In the below paragraphs these steps are explained in further detail by means of a simple example.

System Familiarization

The first step in a fault tree analysis is to get familiar with the system to be analyzed. Before one can construct a fault tree one has to know exactly how the system works and how the various components within the system can fail. If there is only a limited amount of information available on the system under consideration it might be necessary to perform a failure modes and effects analysis to identify all possible failures within the system[17].

To explain the different steps in a fault tree analysis, the safety system as depicted in Figure 6.1 will be analyzed.

The safety system consists of two sensors which for proper functioning require power supply E2. In case the maximum tolerable temperature is exceeded, the sensors send a signal to the one-out of- two logic solver. This logic solver has a different power supply (E1) and in its turn sends a signal to two identical final elements (A1 and A2), which have the same power supply (E2). Only one of the final elements is needed to stop the process and prevent a hazard occurring.

The failure modes to be considered in this example for the various components are:

Sensors	:	Failure to generate a signal given a high temperature
Logic	:	Failure to generate a trip signal to the final elements given one or two trip signals from the sensors
Final elements	:	No action given a demand
Power supply	:	No output

The construciton of a fault tree starts with the definition of the top event. The top event is the top of the fault tree and must be defined unequivocally and can refer to only one specific operational state of the system. After definition of the top event the fault tree has to be constructed. The aim of the fault tree construction is to identify all

causes that contribute to the occurrence of the top event. To construct a fault tree

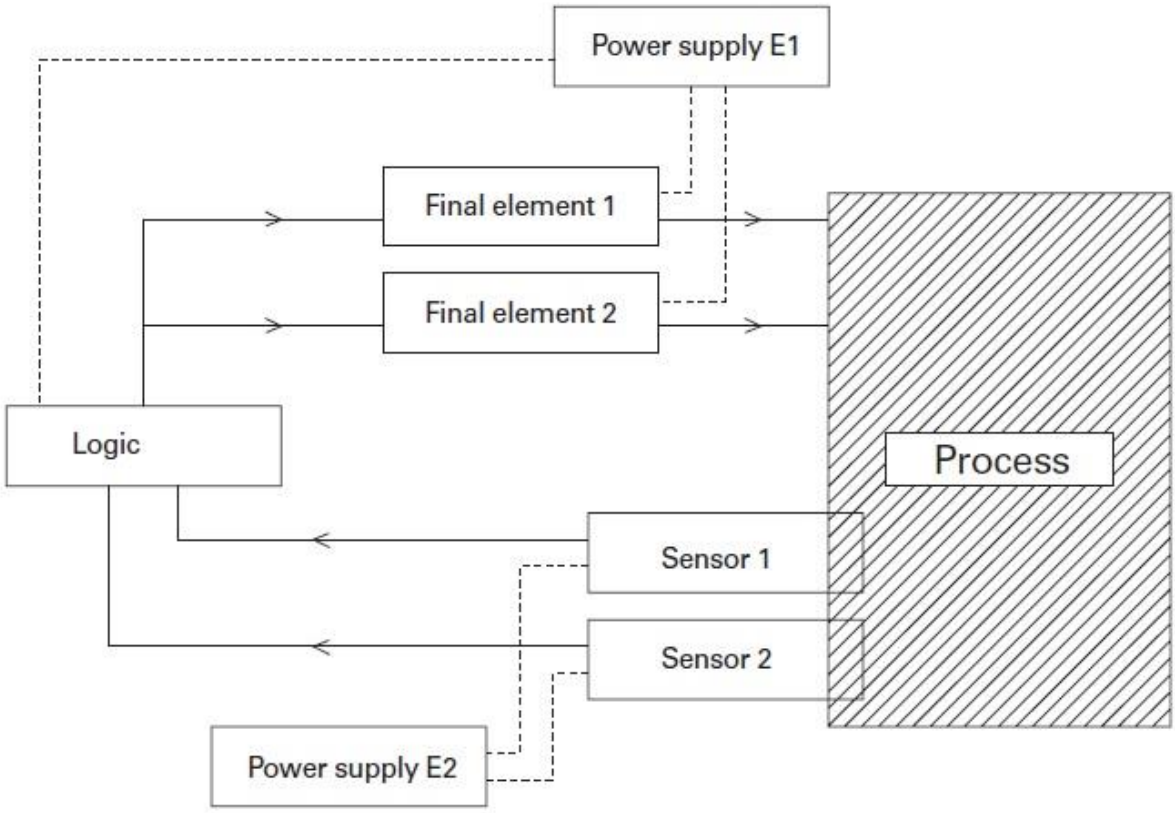


Figure 6.1 : Safety system to be analyzed.

reviewing of system drawings and system descriptions is necessary. Also it is often necessary to consult the supervisor, operator or maintenance crew of the system to identify all contributors to the top event[17].

6.1.3 Fault tree symbology

A fault tree is generated by making a drawing using the symbols depicted in Table 6.1. The construction of a fault tree always starts with the top event as the output of a logic gate. Next, all input events of the ”top event gate” have to be identified. These input events are represented by either new intermediate events or by one or more basic events. In fault trees basic events are end points. New intermediate events are again divided into ”lower” intermediate events and/or basic events. The basic events and intermediate events are mostly joined by ”and” or ”or” gates. This depends on the way in which they influence the output event[18].

The application of the ”AND” and ”OR” gate will be explained with the electrical diagram which is depicted in Figure 6.2.

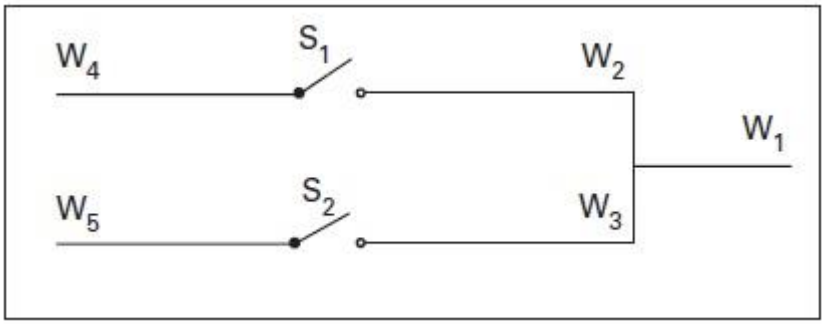


Figure 6.2 : Electrical diagram.

In the electrical diagram of Figure 6.2, there is no power at W1 if there is no power present at W2 and no power present at W3. In a fault tree this fault condition have to be represented by an ”AND” gate. Both input fault events ”No power at W2” and ”No power at W3” have to occur to cause the top event ”No power at W1” to occur. This is depicted in Figure 6.3.

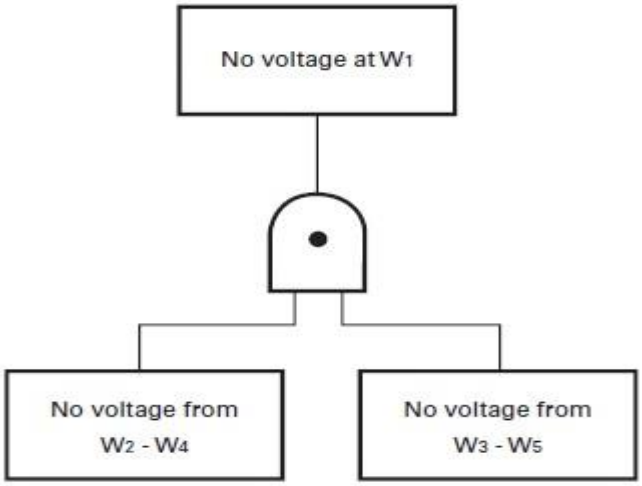


Figure 6.3 : Example of an 'AND' gate.

In the electrical diagram of figure 6.2, there is no power at W2 if switch S1 fails to close or there is no power at W4. In a fault tree this fault condition have to be represented by an ”OR” gate. One out of two input fault events ”Switch fails to close” or ”No power at W4” have to occur to cause the top event ”No power at W2” to occur. This is depicted in Figure 6.5.

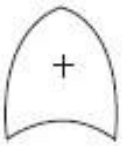
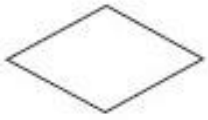
Symbol	Description
	**Intermediate event** A fault event that occurs because of one or more antecedent causes acting through logic gates have occurred.
	**And gate** The AND-gate is used to show that the output event occurs only if all the input events occur.
	**Or gate** The OR-gate is used to show that the output event occurs only if one or more of the input events occur.
	**Basic Event** A basic event that requires no further development because the appropriate limit of resoiution has been reached.
	**Transfer** A triangle indicates that the tree is developed further at the occurrence of the corresponding transfer symbol.
	**Undeveloped Event** A diamond is used to define an event which is not further developed either because it is of insufficient consequence or because information is unavailable.

Figure 6.4 : Fault tree symbols.

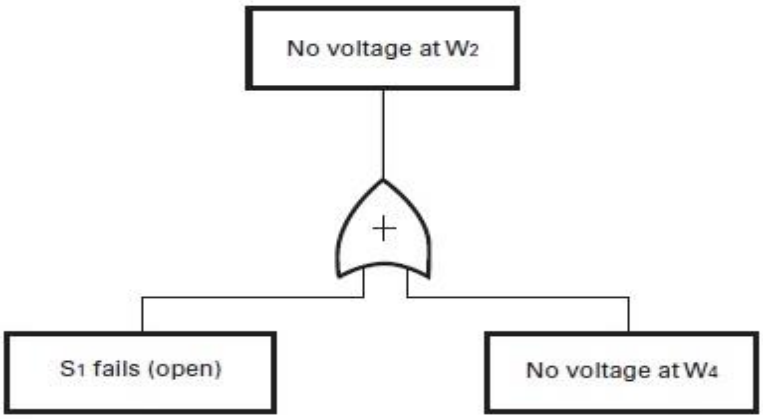


Figure 6.5 : Example of 'OR' gate.

6.1.4 Rules for fault tree construction

Fault tree construction is a process that can be performed in many ways depending on the experience and preferences of the fault tree analyst. To avoid errors in fault tree construction and to give guidance to the fault tree analysts a number of basic rules have been developed. Following these rules a fault tree can be obtained which is correct and easy to understand[19][20].

The rules can be summarized as follows:

Rule 1: Correct definition of top event.

The top event of the fault tree must be defined unequivocally and can refer to only one mode of operation and one specific fault condition of the system.

Rule 2: Construction from top to bottom.

A fault tree is always constructed from top to bottom. One starts with the top event and then works downwards, dissecting the system until one reaches the basic events.

Rule 3: Consistently going upstream.

Given the top event, one must move very consistently upstream through all flow paths. Whether they are electric, hydraulic or pneumatic currents or flows is irrelevant. It will become apparent that there is always some flow to be found. Each component fault is then taken into account. By applying this rule the probability of making errors is decreased as much as possible and components are treated in the right order.

Rule 4: Complete the gate

All inputs into a particular gate should be completely defined before further analysis of any one of them is undertaken.

Rule 5: No gate to gate connections.

Gate inputs should be properly defined fault events, and gates should not be directly connected to other gates.

Rule 6: No miracles.

One might find, in the course of a system analysis, that the propagation of a particular fault sequence could be blocked by miraculous and totally unexpected failure of some other component. For instance it is not allowed to suppose a ”failure to open” of a check valve in the discharge line of a pump after a spurious actuation of the pump. The correct assumption to make is that the component functions normally, thus allowing the passage of the fault sequence in question. However, if the normal functioning of a component acts to block the propagation of a fault sequence, then the normal functioning must be defeated by faults if the fault sequence is to continue up the tree.

Rule 7: Required level of detail

In general it can be stated that the level of detail is sufficient in case the failure data of a certain event is known or if the probability of occurrence of a certain event is negligible compared to the probability of occurrence of the other events.

Fault tree construction example

A fault tree is an organized graphical representation of the conditions or other factors causing or contributing to the occurrence of a defined undesirable event, referred to as the ”top event”.

The corresponding fault tree is depicted in Figure 6.5.

Given rule 2, one needs to start at the point where the safety system interacts with the process. In this example the final elements 1 and 2 stop the process. So this must be the starting point of the fault tree construction. Given that one out of two final elements are required to stop the process, the process is not stopped if both final elements fail to operate. This implies that one has to start with an ”and-gate” because both final elements 1 and 2 have to fail in order to cause the top event to occur.

Two intermediate events can be defined as input event for gate G 1. Final element 1 fails to operate on demand and final element 2 fails to operate on demand. Next, one has to identify all causes why final element 1 is not able to operate. During this investigation one has to move upstream all process flows which are required for proper functioning of final element 1. Three causes can be identified why final element 1 is not able to operate on demand:

- internal failure of final element 1
- no power supply from power supply E1
- no actuation signal from the one-out-of-two logic

The occurrence of each of these three causes is sufficient to cause the intermediate event described by gate G2 to occur. This implies that gate G2 must be an ”or-gate”. The same holds for gate G3.

Three input events have to be drawn for gate G2 and gate G3. Two input events are basic events which describe successively internal failure of the final element and failure of power supply 1. The third input event is the output event of gate G4 which represents the failure of the actuation signal. It must be emphasized that for gate G2 and gate G3 a distinction has to be made between internal failure of final element 1 and internal failure of final element 2. No distinction has to be made between power supply 1 for both gates G2 and G3 because it concerns failure of the same power supply.

A transfer symbol to gate G4 is added to gate G2. This symbol means that the branch represented by the output of G4 is also applicable as input event for G3.

Next, all failure causes of the actuation signal have to be identified. Careful review of the safety system shows that three causes can be identified:

- internal failure of the one-out-of-two logic
- failure of power supply 1
- no signal to the logic from both sensors.

internal failure of the logic is represented by basic event BE4 and failure of the power supply E1 by basic event BE3. Given the design of the logic (one out of two) an ”and-gate” has to be used to describe failure of both actuation signals from the sensors.

Going upstream the signal flow, two different causes can be identified why sensor 1 does not generate an actuation signal. The first cause is an internal failure of the sensor and the second cause is a failure of the power supply E2. So, to describe the failure of sensor 1 to generate an actuation signal, an ”or-gate” G6 has to be added.

Inputs for gate G6 are the basic events BE5 (sensor 1 fails) and BE6 (failure of power supply E2). The same rationale holds for failure of the actuation signal from sensor 2. The complete fault tree is depicted in Figure 6.6[18].

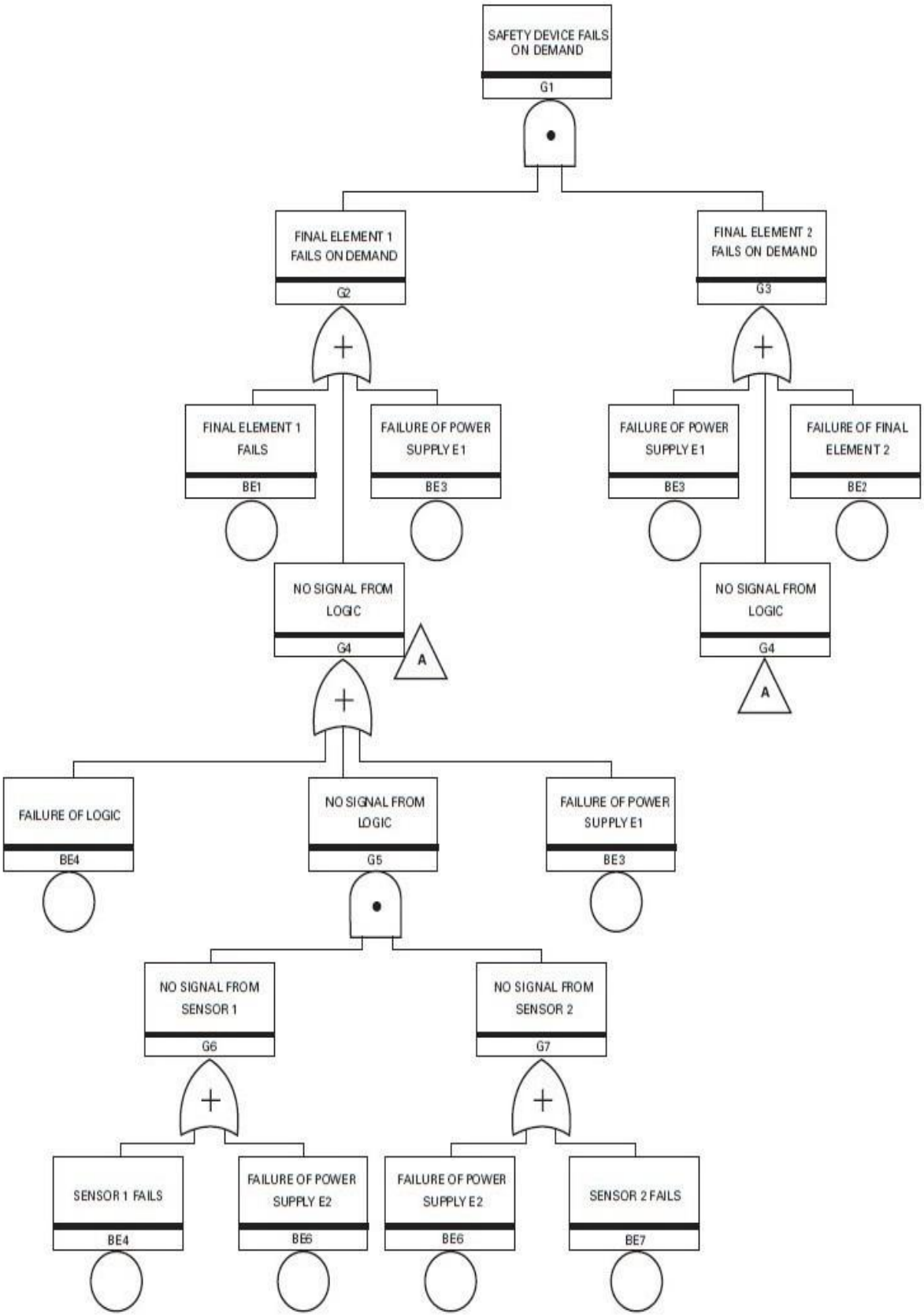


Figure 6.6 : Fault tree safety system.

6.1.5 Application

The strength of fault tree analysis as a qualitative tool is its ability to identify the combinations of equipment failures, dependent failures and human failures that can lead to an undesired consequence. This allows the analyst to focus preventive measures on basic causes to reduce the probability of occurrence. The technique is universally applicable to systems of all kinds[20].

6.1.6 Sofidity

Important limitations of the technique are:
- the presumption that the relevant undesirable events have been identified
- the presumption that contributing factors have been adequately identified and explored in sufficient depth[20].

Apart from these limitations, the technique as usually practised is regarded as being among the most thorough of those prevalent for general system application.

6.1.7 Expertise required

The basis of the fault tree technique is easy to understand and to apply in simple cases. Some years of experience are required to be able to perform a fault tree analysis of a complicated system. Prior knowledge of Boolean algebra and/or the use of logic gates is helpful[20].

6.1.8 Difficulty of application

Application, though time-consuming, is not difficult once the technique has been mastered. Computer aids are available. Unlike Event-Tree Analysis and Failure Modes & Effects Analysis, the technique explores only those faults and conditions leading to the undesired (top) event.

6.2 Markov Processes

6.2.1 Description

A state diagram of a system is constructed. The state diagram represents the status of the system with regard to its failure states. A specific failure state is represented by one node of the state diagram. The arrows between nodes, which represent the failure

events or repair events, are weighted with the corresponding failure rates or repair rates[21].

6.2.2 Application

The Markov technique is most beneficial for analyzing systems where the sequence of failure is important or where repair is done on a continuous basis. The Markov technique can also be applied to the analysis of standby redundancies and state-dependent failure rates. For reliability calculations the Markov process is taken as a discrete-state, continuous-time model. Each discrete state is normally given as a unique, well-defined condition of the relevant system components. In the simplest cases, the formulae which describe the probabilities of the system are readily available in the literature or can be calculated manually. In more complex cases, some methods of simplification can be applied. Results can be calculated also by computer simulation (numerical integration) of the graph.

6.2.3 Sofidity

The Markov technique is one of the most advanced quantitative analysis techniques in risk and reliability analysis. Especially in the case of analyzing different repair strategies the Markov technique is a powerful tool to support the reliability analyst. The disadvantage of this approach is that great care must be taken to eliminate possible dependent events. Dependency can be properly handled by the Markov technique if the system is modelled correctly[22].

6.2.4 Expertise required

The technique is among the more difficult ones. Successful application to complex systems cannot be undertaken without formal study over a period of time, combined with practical experience.

6.2.5 Difficulty of application

Care must be taken to ensure that the state diagram is a realistic representation of the system. If this hurdle is passed, the solution can easily be obtained by the application of a suitable computer code[20].

6.3 Event Tree Analysis

6.3.1 Description

Event trees are used to study or model event sequences which can result in different consequences. The first event of the event sequence is called the initiating event. Depending on the occurrence of one or more intermediate events different outcomes can occur. All possible outcomes relevant to the context of the study are included in the event tree.

The objective of an event tree is to provide insight into the possible consequences of one initiating event which can lead to different consequences, while the objective of fault tree analysis is to clarify how one specific top event, can develop from an indefinite number of basis events[23].

The event trees can be used either for systems in which all components are continuously operating or for systems in which some or all of the components are in a standby mode that involve sequential operational logic and switching. The last type of system is generally associated with safety oriented systems to model accident sequences as the result of a general equipment failure or process upset, the initiating event. For this type of application an event tree analysis is an inductive process where the analyst begins with an initiating event and develops the possible sequences of events that lead to potential accidents.

Although the event tree method is more widely used for safety oriented systems the applications of the technique to both types of systems proceed in a similar manner but with two particular differences between them.

The first is that, with continuously operated systems, the events that can occur, i.e., the components that can fail, can be considered in any arbitrary order. With standby systems, or any system in which the operation of a particular component is dependent on the success or failure of another component, the sequence of events must be considered in the chronological order in which they occur.

The second difference is the starting point of the event tree. In the case of continuously operating systems, the starting point is the system operating normally and the event tree is deduced as a sequence of events involving success and failure of the system components. In the case of standby systems and in particular, safety and mission oriented systems, the event tree is used to identify the various possible

outcomes of the system following a given initiating event which is generally an unsatisfactory operating event or situation.

Event trees have found widespread applications in risk analyses for both the nuclear and chemical industries. These type of applications examines the systems in place that would prevent incidentprecursors from developing into incidents. The event tree analysis of such a system is often sufficient for the purpose of estimating the safety of the system. Human reliability analysis uses event trees to model all possible outcomes of one or more human failures[23].

6.3.2 Event tree analysis methodology

In an event tree there are two types of event to be distinguished, the initiating event and the heading events. An event tree always starts with an initiating event. Other events following that initiating event are called heading or intermediate events.

An initiating event can be recognized from the fact that the various heading events can occur only after occurrences of the initiating event. So the event tree is of interest only if the initiating event has taken place. During the development process of an event tree, conditioned thinking is required. The condition is that at least the initiating event has occurred. The heading events are only of interest after occurrence of the initiating event.

Making an event tree is useful if:

- a specific event can result in more than one outcomes
- one is interested in the probability of occurrence of each of the different outcomes.

More than one outcome implies that several consequences are possible. If this is the case one must always try to make an event tree. For one event and one consequence, a fault tree should be sufficient.

A good event tree offers some very important advantages :

- All possible courses of accidents which can arise from one specific event are arranged in a convenient manner
- An event tree often provides a very good framework for discussions. The point in the tree which is under discussion is clearly defined during discussions. This can then no longer be misinterpreted and the impatient can see whether or not their problem is coming up for discussion (at a different point in the tree)

- As soon as the principle of the event tree is known, everybody can understand why certain events do occur and why other combinations of events do not occur.

In an event tree analysis at least two branches have to be considered for each heading event which plays a role in the accident sequence under consideration.[24].

6.3.3 Construction of an event tree

The construction of an event tree, considering a specific initiating event, starts with the collection of all relevant heading events. The next step is to put the heading events in the right order. For safety applications the heading events are put in chronological order in accordance with the activation of the various safeguarding systems or physical processes which might occur after occurrence of the initiating event. Starting from the initiating even, event sequences are developed by defining branches for each relevant heading event. If the occurrence of a specific heading event does not influence the event sequence under consideration no branch is defined for that specific heading event. It should be emphasized that one can define more than two branches for a specific heading event if necessary. The only boundary condition is that the enumeration of all branch probabilities must be equal to one[25].

Nomenclature

A - Initiating event
B - Heading event
C - Heading event
D - Heading event
E - Heading event
F - Heading event

B* - Heading event B does not occur
C* - Heading event C does not occur
D* - Heading event D does not occur
E* - Heading event E does not occur
F* - Heading event F does not occur

P - Probability

P(A) - Probability of iniating event A for one year of operation

P(B) - Conditional probability of event B

P(C) - Conditional probability of event C

P(D) - Conditional probability of event D

P(E) - Conditional probability of event E

P(F) - Conditional probability of event F

6.3.4 Event tree quantification

The quantification of an event tree will be explained will an example. The example is a postincident analysis of a large leakage of pressurized flammable material from an isolated LPG storage tank. An HAZOP analysis indicates that the potential consequences include BLEVE (Boiling Liquid Expanding Vapor Explosion) of the tank if the leak is ignited (either immediately or by flashback). If the leak does not immediately ignite, the cloud can drift away. The cloud can be ignited in that case by several ignition sources and explode UVCE (Unconfined Vapor Cloud Explosion), or produce a flash fire some time later. An event tree is developed to predict possible outcomes from the leakage of LPG. The event tree is depicted in Figure 6.7.

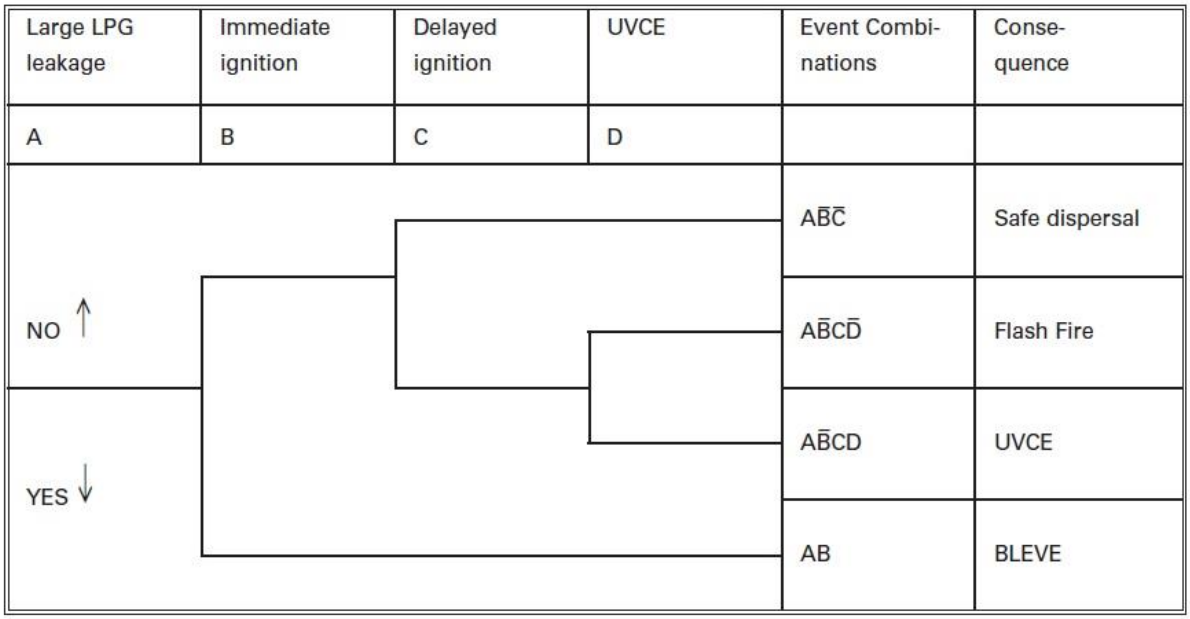


Figure 6.7 : Event tree for the LPG leakage initiating event.

The heading events are defined as follows:

A: Large LPG leakage from vessel (Initiating event)

B: Immediate ignition

C: Delayed ignition

D: Unconfined Vapor Cloud Explosion

B* - Heading event B does not occur

C* - Heading event C does not occur

D* - Heading event D does not occur

A total of four outcomes are identified: a Boiling Liquid Expanding Vapor Vapor Explosion, A Unconfined Vapor Cloud Explosion, a Flash or Safe dispersal.

Assuming independence between the various heading events, the probability of occurunce of the different consequences can be calculated with the following formulas:

P(Safe dispersal) = P(A) * (1-P(B)) * (1-P(C))

P(Flash Fire) = P(A) * (1-P(B)) * P(C) * (1-P(D))

P(UVCE) = P(A) * (1-P(B)) * P(C) * P(D)

P(BLEVE) = P(A) * P(B)

Suppose that the following data is valid for this situation:

P(A) = 5.0E-07 for one year of operation

P(B) = 0.7 -

P(C) = 0.7 -

P(D) = 0.1 -

P(Safe dispersal) = 5.0E-07 * (1 - 0.7) * (1 - 0.7)

= 4.5E-08 for one year of operation

P(Flash Fire) = 5.0E-07 * (1 - 0.7) * 0.7 * (1 - 0.1)

= 9.8E-08 for one year of operation

P(UVCE) = 5.0E-07 * (1 - 0.7) * 0.7 * 0.1

= 1.05E-08 for one year of operation

P(BLEVE) = 5.0E-07 * 0.7

= 3.5E-07 for one year of operation

The total frequency of all outcomes is a check to ensure that this equals the initiating event frequency of 5.0E-07 per year.

6.3.5 Event tree development procedure

The construction of an event tree is sequential, and like fault tree analysis, is top-down (left-right in the usual event tree convention). The construction begins with the initiating event, and the temporal sequences of occurrence of all relevant safety functions or events are entered. Each branch of the event tree represents a separate outcome (event sequence). The process of event tree development can be divided in a number of steps. A concise description of each step will be provided: [24][25].

Step 1 : ldentification of the initiating event.

The initiating event, in many quantitative risk assessments, is a failure event corresponding to a release of hazardous material or a plant disturbance which can lead to serious consequences if one or more safety devices fail. The initiating event might correspond to a pipe leak, a vessel rupture, an internal explosion, etc.

Step 2: ldentification of safety function/ Hazard Promoting Factor and Outcome definition.

A safety function is a device, action, or barrier, that can interrupt the sequence from an initiating event to a hazardous outcome. A hazard promoting factor may change the final outcome (e.g., from a dispersion cloud to a flash fire or to a UVCE).

Step 3: Construction of event tree.

The event tree graphically displays the chronological progression of an incident. Starting with the initiating event, the event tree is constructed left to right. At each heading or node two or more alternatives are analysed until a final outcome is obtained for each branch. Only nodes that materially affect the outcome should be shown explicitly in the event tree. Some branches may be more fully developed than others. In pre-incident analysis, the final sequence might correspond to successful termination of some initiating events or a specific failure mode. The listing of the safe recovery and incident conditions is an important output of this analysis. For a post-incident analysis, the final result might correspond to the type of incident outcome. The event heading should be indicated at the top of the page, over the appropriate branch of the event tree. If possible the heading events should describe the undesired situation. It is usually to have the YES branch downward and the NO branch upward. Starting with the initiating event, each heading event is labelled with a letter identifier. Every final event sequence can then be specified with a unique

letter combination. A bar over the letter indicates that the designated event did not occur.

Step 4: Classify the outcomes.

The objective in constructing the event tree is to identify important possible outcomes that are important contributors to risk to be quantified. Thus, if an estimated of the risk of offsite fatalities is the goal of the analysis, only outcomes relevant to that outcome need be developed. Branches leading to lesser consequences can be left undeveloped. Many outcomes developed through different branches of the event tree will be similar. The final event tree outcomes can be classified according to type of consequence model that must be employed to complete the analysis.

Step 5: Estimation of the conditional probability of each branch in the event tree.

The each heading in the event tree (other than the initiating event) corresponds to a conditional probability of some outcome if the preceding event has occurred. Thus, the probabilities associated with each limb must sum to 1.0 for each heading. This is true for either binary or multiple outcomes from a node. The source of conditional probabilities may be historical records, plant and process data, equipment reliability data, human reliability data, expert opinion. It may be necessary to use fault tree techniques to determine some probabilities, especially for complex safety systems in pre-incident analysis.

Step 6: Quantification of the outcomes.

The frequency of each outcome may be determined by multiplying the initiating event frequency with the conditional probabilities along the path leading to that outcome. It should be emphasized that this type of quantification is only allowed if the initiating event frequency and the conditional probabilities can be considered all as independent events.

Step 7: Evaluation.

The results of the event tree analysis should be tested with common sense and against system or process understanding and historical records. Dominant contributors to risk can be identified and recommendations to decrease the risk level can be formulated.

6.3.6 Application

The technique is universally applicable to systems of all kinds, with the limitation that unwanted events (as well as wanted events) must be anticipated to produce meaningful analytical results.

6.3.7 Sofidity

The technique can be exhaustively thorough, Solidity has only two theoretical limits, i.e. the presumptions that:
- all system events have been anticipated
- all consequences of those events have been explored.

6.3.8 Expertise required

The technique is among the more difficult. Successful application to complex systems cannot be undertaken without formal study over a period of time, combined with practical experience.

6.3.9 Difficulty of application

The technique is not particularly difficult to apply. It is, however, time-consuming. It must be recognized that the exploration of all wanted events and their consequences increases the effort substantially.

6.4 Monte Carlo Simulation

6.4.1 Description

Some practical problems in risk and reliability analysis cannot be solved by analytical methods and require numerical simulation. Thus, rather than attempt to analytically analyse the effects on inputs described with probability distributions, e.g. failure rates of components, Monte Carlo techniques represent the distributions as sequences of discrete random values. The technique consists of building, usually with a computer code, a probabilistic model of the system under investigation. A trial run of the model is repeated many times, and each time one discrete value of the performance of the simulated system is recorded. After a sufficiently large number of computer runs, these discrete values can be combined into one probability distribution which describes the system parameter of interest[26].

6.4.2 Application

The technique requires the building of a probabilistic model of the system, translation of this model into a computer model, estimation of the probability distributions of the input parameters and composition and interpretation of the output probability distribution. It will be clear that this is a time-consuming process and requires various skills. For this reason it is advisable to use the Monte Carlo technique only in those cases where analytical methods fail.

6.4.3 Sofidity

Very realistic results can be generated with the Monte Carlo technique. Almost all aspects can be incorporated into the probabilistic model.

6.4.4 Expertise required

Analysts need to be familiar with system reliability techniques and need to have a detailed understanding of probability distributions. In most cases some computer programming is necessary to model the probabilistic system model. Interpretation of the results requires analysts to be familiar with median, mean and upper and lower bounds of probability distributions.

6.4.5 Difficulty of application

The analyst must be familiar with probability distribution and random number generators. Also some computer programming is required in most cases.
In the case of very reliable systems a large number of computer runs are required to generate a probability distribution. New techniques have been developed to save computer time[26].

7. EXPLOSION

An explosion involves the production of a pressure discontinuity or blast wave resulting from a rapid release energy. A pressure disturbance is generated in to the surrounding medium. Air becomes heated due to its compressibility and this leads to an increase in the velocity of sound, causing the front of distrubance to steepen as it travels through the air. The loading and hence the damge to the nearby targets are governed by the magnitude of and duration of pressure waves. Missiles may be generated by an explosion and are capable of causing severe damage to adjacent plant structures and people. The explosions mainly occurs due to the rapid combustion of a flammable material but can be brought about the chemical reactions other than combustion, provided they release large amount of energy (heat)[27].

Classification of Explosions

- Chemical Explosions
- Physical Explosions
- Vapour Cloud Explosions

7.1 Chemical Explosion

Chemical explosions in plant or in vessel can arise due to exothermic reaction occurring internally. Such reaction may involve decomposition of unstable substances, polymerization of monomers, or combustion of fuel oxidant mixtures. Heating and increase of molecular number can result in a rise in pressure to the bursting point of the vessel, and exlosives decompose so quickly that confinement and development of pressure are self – imposed[27].

7.2 Physical Explosion

It occurs simply due to over pressure as in the case of steam boiler and air receiver explosions. Fire is not necessarily a consequence. But fire involving stock, buildings and plant ancillaries can cause physical explosions due to overheating followed by overpressure in vessels and also the fireballs if contents are flammable. One such case is termed as Boling Liquid Expanding Vapour Explosion (BLEVE)[27].

7.2.1 BLEVE

BLEVE – (Boiling Liquid Expanding Vapor Explosion) occurs when a vessel containing liquid under pressure, such as a liquid propane tank, is subjected to a temperature above the liquid's boiling point. If heat raises the pressure inside the sealed tank to the point where the vessel can no longer contain the pressure, the vessel will mechanically fail and a BLEVE will occur. If the liquid inside the tank is flammable a fire will often ensue. If not, the BLEVE will still occur, but the vapors will not ignite (a steam boiler is a common example of this). BLEVEs can also be caused by mechanical damage or overfilling[28].

The boiling liquid expanding vapour explosion (BLEVE) happens when a vessel holding a pressure liquefied gas (PLG) fails catastrophically. The vessel failure may be due to:

- Severe fire exposure
- Severe overpressure
- Severe corrosion
- Severe mechanical impact
- Severe manufacturing flaw
- Or a combination of all of the above

A pressure liqufied gas (PLG) is normally at vapour at ambient pressure and temperature but is stored as a liquid under pressure at ambient temperature. If the containment is suddenly lost then the liquid is sent to into state of superheat, and this can lead to sudden and violent phase change of a large fraction of the liquid. The BLEVE is the explosive release of expanding vapour and flashing liquid. Hazards from a BLEVE include blast overpressure, projectiles, possible toxic release and if flammable a fireball, flash fire or a vapour cloud explosion (VCE)[29].

Overpressure :

Overpressure, also called blast wave, refers to the sudden onset of a pressure wave after an explosion. This pressure wave is caused by the energy released in the initial explosion – the bigger the initial explosion, the more damaging the pressure wave. Pressure waves are nearly instantaneous, traveling at the speed of sound. Although a pressure wave may sound less dangerous than a fire or a toxic cloud, it can be just as damaging and just as deadly. The pressure wave radiates outward and generates

hazardous fragments (such as building debris and shattered glass). Additionally, these waves can damage buildings or even knock them flat – often organs like the ears and lungs. The below table relates overpressure values to the structural and physiological effects produced[30].

Table 7.1 : Expected damage by overpressure.

Overpressure* (psig)	Expected Damage
0.04	Loud noise (143 db); sonic boom glass failure.
0.15	Typical pressure for glass failure.
0.40	Limited minor structural damage.
0.50-1.0	Windows usually shattered; some window frame damage.
0.70	Minor damage to house structures.
1.0	Partial demolition of houses; made uninhabitable.
1.0-2.0	Corrugated metal panels fail and buckle. Housing wood panels blown in.
1.0-8.0	Range for slight to serious laceration injuries from flying glass and other missiles.
2.0	Partial collapse of walls and roofs of houses.
2.0-3.0	Non-reinforced concrete or cinder block walls shattered.
2.4-12.2	Range for 1-90% eardrum rupture among exposed populations.
2.5	50% destruction of home brickwork.
3.0	Steel frame buildings distorted and pulled away from foundation.
5.0	Wooden utility poles snapped.
5.0-7.0	Nearly complete destruction of houses.
7.0	Loaded train cars overturned.
9.0	Loaded train box cars demolished.
10.0	Probable total building destruction.
14.5-29.0	Range for 1-99% fatalities among exposed populations due to direct blast effects.
* These are peak pressures formed in excess of normal atmospheric pressure by blast and shock waves.	

Lees, Frank P. 1980. *Loss Prevention in the Process Industries*, Vol. 1. London and Boston: Butterworths.

7.3 Vapour Cloud Explosion

A vapor cloud explosion is a process where a combustion of a premixed gas results in a rapid increase in pressure. Before a vapor cloud explosion is possible, there are several events that must occur. These events are illustrated in Figure 7.1. As the figure shows, it is essential to have a release of gas in order to have an explosion. Secondly, ignition must be present to ignite the released gas, which could result in fire or an explosion[31].

Vapour cloud explosions can take place in buildings or offshore modules, inside process equipment or pipes, in open process areas, or in unconfined areas. The vapor

cloud explosions are classified based on the environment in which the explosion occurs. There are generally three types of explosions[31]:

- Confined gas explosions within vessels, pipes, channels or tunnels
- Partly confined gas explosions in compartments, buildings or offshore modules.
- Unconfined gas explosions in process plants and other unconfined areas.

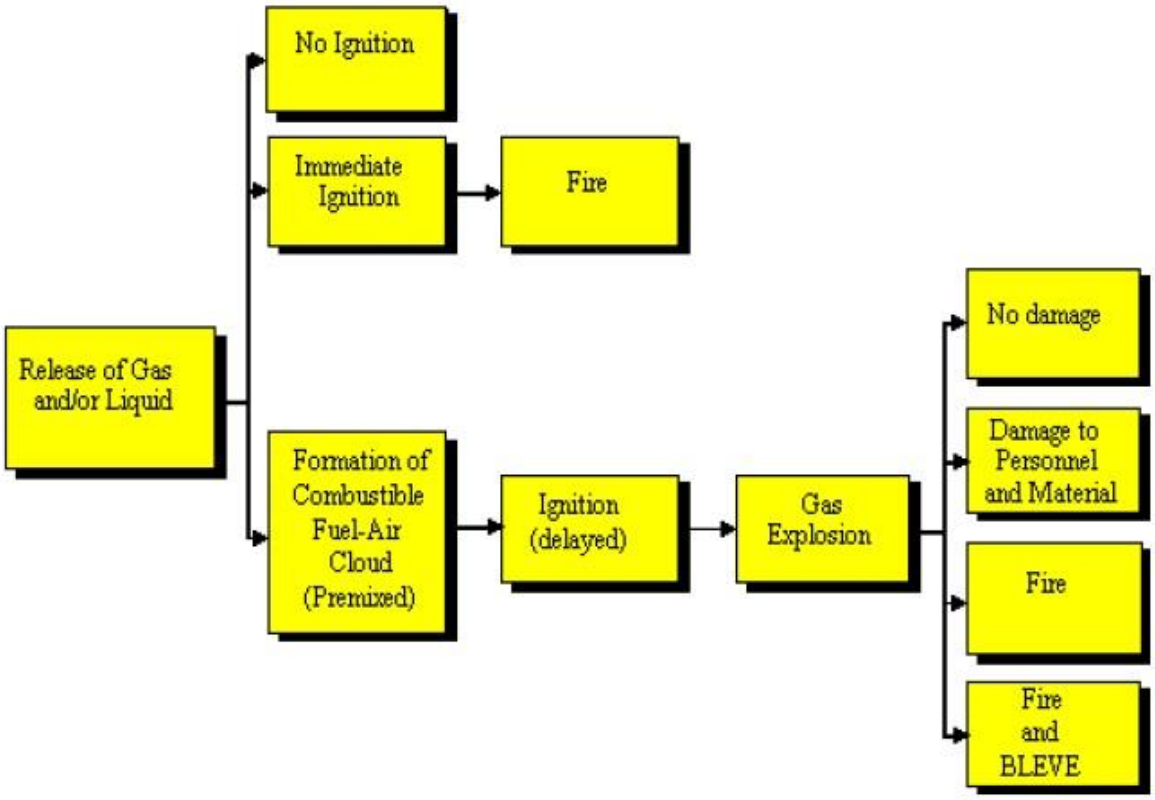


Figure 7.1 : Events leading to gas explosion, BLEVE - boiling liquid expanding vapour explosion.

An unconfined vapour cloud explosion in a processing plant can involve partly confined explosions in closed modules or highly congested areas where the vapor cloud has leaked. Confined vapour cloud explosions, so called internal explosions, are explosions which take place within processing equipment, tanks, pipes, sewage systems, culverts, and closed rooms. The combustion process in this kind of explosion does not need to be quick to result in a severe pressure increase. Partly confined explosions take place when flammable material is accidentally discharged inside a building which is partly open, such as compressor rooms and offshore modules. The building will contain the explosion but the explosion overpressure can only be relieved through the explosion vent panels, or through breakdown of the surrounding walls [31].

Unconfined vapor cloud explosions take place in open areas such as hydrocarbon and petrochemical processing plants. It has been demonstrated in large-scale tests that an actually unconfined, unobstructed flammable vapor cloud ignited by a weak ignition source will lead to flash fire. In a real hydrocarbon processing plant, however, there are partly confined and obstructed local areas such as pipe racks which could cause deflagration with high overpressures. A deflagration has a limited burning velocity, in the range 100–500 m/s. On the other hand, if an unconfined vapor cloud detonates, the resulting overpressure will be very high, in the order of 20 bars. Most vapor cloud explosions on onshore and offshore hydrocarbon processing plants would fall into the category of deflagrations [31].

7.3.1 Vapor cloud explosion modelling

When examining the vapor cloud explosion overpressure prediction methodologies, it was found that there exist different models which vary from simple empirical models to more sophisticated and complex models. These models have been classified as follows:

- Empirical models: These models are based on correlations developed from analysis of experimental data. They are considered very simple models and their applicability is very limited. In addition, these models cannot handle complex geometries and as a result, they have significantly simplified the physics. Despite all aforementioned limitations, these models can be usefully used for quick order-of-magnitude calculations and for screening purposes for more analysis with more complex models.
- Phenomenological models: These models are slightly more complex and have a broader range of applicability than the previous models. These models are based on differential and algebraic equations which describe the physical process involved in the vapor cloud explosions. These models can model certain types of geometry by representation of an idealized system. In terms of sophistication, phenomenological models are somewhere between empirical models and complex Computational Fluid Dynamics models. These type of models has short running times and can run a large number of different scenarios.

- Computational Fluid Dynamic (CFD) models: CFD models find the numerical solutions of the Navier-Stokes equations which govern the fluid flow. The numerical solutions are developed by discretizing the solution domain in both space and time. CFD has a wide range of applicability and can be used in many different disciplines. When comparing CFD with empirical and phenomenological models, CFD provides greater flexibility and accuracy. However, the main limitations of CFD are the process run time and the complexity of using it [31].

8. TOXIC RELEASE

The prevailing wind speed and the weather conditions play the important role in determining the dimensions of the toxic plume. To understand exposure limits and their respective effects we can divide the affected area in to three zones of various concentration levels. The table describes the limits and effects [32].

Table 8.1 : Toxic release effects and limits.

Concentration Level	Observed Effects
Short -Term Exposure Limit (STEL) Blue Zone	Maximum concentration of the substance to which workers can be exposed for a period up to 15 minutes without suffering (a) Intolerable Irritation (b) Chronic or irreversible tissue change (c) narcosis of sufficient degree to increase accident proneness, impair self rescue, or materially reduce worker efficiency, provided that no more than 04 excursion per day are permitted, with at least 60 minutes between exposure periods, and provided that daily TLV is not exceeded. It should not be used to evaluate the toxic exposure upto 30 minutes.
Immediately Danger to Life and Health (IDLH) Orange Zone	An atmospheric concentration of any toxic, corrosive or asphyxiant sustance that poses an immediate threat to life or would cause irreversible or delayed adverse health effects or would interfere with an individual's ability to escape from a dangerous atmosphere. If IDLH values are exceed, all unprotected people must elave the area immediately. The maximum airborne concentration of a susbtance to which a worker is exposed for long as 30 minutes and still be able to escape without loss of life.
Lethal Concentration at 50% mortality (LC50) Red Zone	LC stands for 'Lethal Concentration'. LC values usually refer to the concentration of a chemical in air but in environmental studies it can also mean the concentration of a chemical in water. For inhalation experiments, the concentration of the chemical in air that kills 50% of the test animals in agiven time (usually half to four hours) is the LC_{50} value.
Fatal Level	Death

9. FIRE

The Fire is a process of burning that produces heat, light and often smokes and flames. The effect of fire on the people takes the form of skin burn due to the exposure to thermal radiation. The severity of the burns depends upon the intensity of the heat and exposure time. In general terms the skin withstands heta energy of 10Kw/m^2 for approximately 8 seconds and that of 30kW/m^2 for 0.4 seconds before pain is felt. The effect of various heat radiation levels is given in the table below [33].

Table 9.1 : Radiation effects.

Radiation Level (kW/m^2)	Observed Effect
37.5 (Red zone)	Sufficient to cause damage to process equipment
25	Minimum energy required to ignite wood at indefinitely long exposures (non-piloted)
12.5 (Orange zone)	Minimum energy required for piloted ignition of wood, melting of plastic
10	Pain threshold reached after 8 second; second degree burns after 25 second
4,7	Accepted value to represent injury
4 (Blue zone)	Sufficient to cause pain to personnel if unable to reach cover within 20 seconds; however blistering of the skin (second degree burns) is likely;0: lethality
1,6	Will cause no discomfort for the long exposure

Fire can takes several different forms i.e.

- Flash Fire
- Jet Fire
- Pool Fire
- Secondary Fire

9.1 Flash Fire

A flash fire occurs when a cloud of flammable gas and air is ignited. The speed of burning is function of the concentration of the flammable component in the cloud and also the wind speed. Within a few second of ignition the flame spreads both upwind and downwind of the ignition source. Initially the flame is contained with in the cloud due to premixed burning of the regions within the flammable limits. Subsequnetly the flame extends in the form of a fire plume above the cloud. The downwind edge of the flame starts to move towards the spill point after consuming the flammable vapor downwind of the ignition source. The duration of this fire is very short and damage is caused by thermal radiation and oxygen depletion [33].

9.2 Jet Fire

A jet fire occurs when a flammable liquid or gas is ignited after its release from a pressurized, punctured vessel or pipe. The pressure of release generates a long flame, which is stable under most conditions. A flash flame may take the form of jet flame on reaching the spill point. The duration of the jet fire is determined bt the release rate and capcity of the source. Flame length increases directly with flow rate. Typically a pressuized release of 8kg/s would have a length of 35m. The cross winds also affects the flame length [33].

9.3 Pool Fire

A pool fire occurs on ignition of an accumulation of liquid as a pool on the ground or on water or other liquid. A steadily burning fire is rapidly achieved as the flame vapour to sustain the fire is provided by evaporation of liquid by heat from the flames. The maximum burning rate is function of the net heat of combustion and heat required for its vaporization. Generally heat radiation dominates the burning rate for lame greater than 1m diameters. Big pool fire is hazardous and disastrous to control it. This type of fire is prominent in tank farm areas and in bulk depots of petroleum products where petrol, diesel are stored. Jaipur fire of the 2009 was the worst example of pool fire in Indian history where we lost petroleum products of worth crores and human lives and property. District collectors have to audits such bulk

depots from disaster prevention angle and should be in the priority list of their administration [33].

9.4 Secondary Fire

The secondary fire involves the combustion of flammable materials those are not directly concerned with the process, and some time present unnecessarily. For example :

- Stored raw material and procducts, including packaging materials;
- Combustile insulation of vessels, pipelines and electrical cables;
- Combustile building material and linings.

Protection is by elimination or segregation of combustile materials, use of incombustible materials of construction and insulation, and control of ignition sources. Careless or deliberate actions may defeat in-built precautions[33].

10. OIL SPILLS AND DISASTERS

The following list includes major oil spills since 1967. The circumstances surrounding the spill, amount of oil spilled, and the attendant environmenta damage is also given.

- 1967 March 18, Cornwall, Eng.: Torrey Canyon ran aground, spilling 38 million gallons of crude oil off the Scilly Islands
- 1976 December 15, Buzzards Bay, Mass.: Argo Merchant ran aground and broke apart southeast of Nantuclet Island, spilling its entire cargo of 7.7 million gallons of fuel oil.
- 1977 April, Nort Sea: blowout of well in Ekofisk oil field leaked 81 million gallons.
- 1978 March 16, off Portsall, France: wrecked supertanker Amoco Cadiz spilled 68 million gallons, causing widespread environmental damage over 100 mi of Brittany coast.
- 1979 June 3, Gulf of Mexico: exploratory oil well Ixtoc 1 blew out, spilling an estimated 140 million gallons of crude oil into the open sea. Although it is one of the largest known oil spills, it had a low environmental impact
- 1979 July 19, Tobago: the Atlantic Empress and Aegean Captain collided, spilling 46 million gallons of crude. While being towed, the Atlantic Empress spilled an additional 41 million gallons off Barbados on Aug.2.
- 1980 March 30, Stavanger, Norway: floating hotel in North Sea collapsed, killing 123 oil workers.
- 1983 February 4, Persian Gulf, Iran: Nowruz Field platform spilled 80 million gallons of oil.
- 1983 Aug.6, Cape Town, South Africa: the Spanish tanker Castillo de Beliver caught fire, spilling 78 million gallons of oil off the coast.
- 1988 July 6, North Sea off Scotland: 166 workers killed in eplosion and fire on Occidental Petroleum’s Piper Alpha rig in North Sea; 64 survivors. It is the world’s worst offshore oil disaster.

- 1988 November 10, Saint John's, Newfoundland: Odyssey spilled 43 million gallons of oil.
- 1989 March 24, Prince William Sound, Alaska: tanker Exxon Valdez hit an undersea reef and spilled 10 million – plus gallons of oil into the water.
- 1989 December 19, off Las Palmas, the Canary Islands: explosion in Irarian supertanker, the Kharg-5, caused 19 million gallons of crude oil to spill into Atlantic Ocean about 400 mi north of Las Palmas, forming a 100-square-mile oil slick.
- 1990 June 8, off Galveston, Texas: Mega Borg released 5.1 million gallons of oil some 60 nautical miles south-southeast of Galveston as a result of an explosion and subsequent fire in the pump room.
- 1991 January 23-27, southern Kuwait: during the Persian Gulf War, Iraq deliberately released 240-460 million gallons of crude oil into the Persian Gulf from tankers 10 mi off Kuwait. Spill had little military significance. On january 27, U.S. warplanes bombed pipe systems to stop the flow of oil.
- 1991 April 11, Genoa, Italy: Heaven spilled 42 million gallons of oil in Genoa port.
- 1991 May 28, Angola: ABT Summer exploded and leaked 15-78 million gallons of oil off the coast of Angola. It's not clear how much sank or burned.
- 1992 March 2, Fergana Valley, Uzbekistan: 88 million gallons of oil spilled from an oil well.
- 1993 August 10, Tampa Bay, Fla.: three ships collided, the barge Bouchard B155, the freighter Balsa 37, and the barge Ocean 255. The Bouchard spilled an estimated 336,000 gallons of No.6 fuel oil into Tmapa Bay.
- 1994 September 8, Russia: dam built to contain oil burst and spilled oil into Kolva River tributary.U.S. Energy Department estimated spill at 2 million barrels. Russian state-owned oil company claimed spill was only 102,000 barrels.
- 1996 February 15, off Welsh coast: supertanker Sea Empress ran aground at port of Milford Haven, Wales, spewed out 70,000 tons of crude oil, and created a 25-mile slick.

- 1999 December 12, French Atlantic coast: Maltese-registered tanker Erika broke apart and sank off Britanny, spilling 3 million gallons of heavy oil into the sea.
- 2000 January 18, off Rio de Janerio: rupture pipeline owned by government oil company, Petrobas, spewed 343,200 gallons of heavy oil into Guanabara Bay.
- 2000 November 28, Mississippi River south of New Orleans: oil tanker Westchester lost power and ran aground near Port Sulphur, la., dumping 567,000 gallons of crude oil into lower Mississippi. Spill was largest in U.S. waters since Exxon Valdez disaster in March 1989.
- 2002 November 13, Spain: Prestige suffered a damaged hull and was towed to sea and sank. Much of the 20 million gallons oil remains underwater.
- 2003 July 28, Pakistan: The Tasman Spirit, a tanker, ran aground near the Karachi port, and eventually cracked into two pieches. One of its four oil tanks burst open, leaking 28,000 tons of crude oil into the sea.
- 2004 December 7, Unalaska, Aleutian, Alaska: A major storm pushed the M/V Selendang Ayu up onto a rocky shore, breaking it in two. 337,000 gallons of oil were released, most of which was driven onto the shoreline of Makushin ans Skan Bays.
- 2005 Aug.-Sept.,New Orleans, Louisiana: The coast Guard estimated that more 7 million gallons of oil were spilled during Hurricane Katrina from various sources, including pipelines, strorage tanks and industrial plants.
- 2006 June 19, Calsasieu River, Louisiana: An estimated 71,000 barrels of waste oil were released from a tank at he CITGO Refinery on the Calcasieu River during a violent rain storm.
- 2006 July 15, Beirut, Lebanon: The Israeli navy bombs the Jieh coast power station, and between three million and ten million gallons of oil leaks into the sea, affecting nearly 100 miles of coastline. A coastal blockade, a result of the war, greatly hampers outside clean-up efforts.
- 2006 August 11th, Guimaras island, The Philippines: A tanker carrying 530,000 gallons of oil sinks off the coast th Philippines, putting the country's fishing and tourism industries at great risk. The ship sinks in deep water,

making it virtually unrecoverable, and it contiunes to emit oil into the ocean as other nations are called in to assist in the massive clean-up efforts.

- 2007 December 7, South Korea: Oil spill causes environmental disater, destroying beaches, coating birds and oysters with oil, and driving away tourists with its stench. The Hebei Spirit collides with a steel wire connecting a tug boat and barge five miles off South Korea's west coast, spilling 2.8 million gallonns of crude oil. Seven thousand people are trying to clean up 12 miles of oil-coated coast.
- 2008 July 25, New Orleans, Louisiana: A 61-foot barge, carrying 419,000 gallons of heavy fuel, collides with a 600-foot tanker ship in the Mississippi River near New Orleans. Hundreds of thousands of gallos of fuel leak from the barge, causing a halt to all river traffic while cleanup efforts commence to limit environmental fallout on local wildlife.
- 2009 March 11, Queensland, Australia: During Cyclone Hamish, unsecured cargo aboard the containes ship MV Pacific Adventurer came loose on deck and caused the release of 52,000 gallons of heavy fuel and 620 tons of ammonium nitrate, a fertilizer, into the Coral Sea. About 60 km of Sunshine Coast was covered in oil, prompting the closure of half the area's beaches.
- 2010 January 23, Port Arthur, Texas: The oil tanker Eagle Otome and a barge collide in the Sbaine-Neches Waterway, causing the release of about 462,000 gallons were recovered and 175,000 gallons were disperdes or evaporated, according to th U.S. Coast Guard.
- 2010 April 24, Gulf of Mexico: The Deepwater Horizon, a semi-submersible drilling rig, sank on Aprill 22, after an April 20th explosion on the vessel. Eleven people died in the blast. When the rig sank, the riser – 5,000-foot-long pipe thah connects the wellhead to the rig – became detached and began leaking oil. In addtion, U.S. Coast Guard investigators discovered a leak in the wellhead itself. As much as 60,000 barrels of oil per day were leaking into the water, threating wildlife along the Louisiana Coast. Homeland Security Secretary Janet Napolitano declared it a 'spill of national significance.' BP (British Petroleum), which leased the Deepwater Horizon, is reponsible for the cleanup, but he U.S. Navy supplied the company with resources to help contain the slick. Oil reached the Louisiana shore on April

30, affected about 125 miles of coast. By early June, oil had also reached Florida, Alabama and Mississippi. It is the largest oil spill in U.S. history [34].

11. THE PETROLEUM PIPELINE CORPORATION (BOTAS)

The Petroleum Pipeline Corporation (BOTAS) was established on 15 August 1974 to trasnport crude oil. Since 1987 it has engaged in natural gas transportation and trade activities as well and has become the leading company in natural gas and crude oil sectors. The main activities of BOTAS are crude oil and natural gas trasnportation and pipeline operation as well marine terminal operations. The plant contain thirteen crude oil strorage tanks. One of the tank is always empty for emergency situations. The strorage tank volume capcity are different. Three of them capacity are 50000 m^3 and the others are 135000 m^3. The maximum discharge velocity of crude oil to tank is 4500m^3/hour and maximum load velocity of crude oil from tank to ship is 13000m^3/hour. The average temperature of crude oil is between 62-65 °F and the gravity is API 34.40.

The purpose of this study for this plant to

- Calculate and show potential risk profiles of plant with the following major hazard scenarios.
- Analyse the profiles;
- Determine and prepare emergency plans for these scenarios.

11.1 BOTAS Hazard Scenarios

Scenario 1 – A catastrophic leak from pipeline connection point to the crude oil storage tank .

Tank volume : 135,000 m^3 ; Tank height : 17 m; Tank diameter : 100 m; Diameter of pipe : 30 inch ; Discharge velocity to the tank : 4500 m^3/hour ;

Scenario 2 – A small leakage (1 % pipe area) from pipeline connection point to the crude oil storage tank .

Tank volume : 135,000 m^3 ; Tank height : 17 m; Tank diameter : 100 m; Diameter of pipe : 30 inch ; Discharge velocity to the tnak : 4500 m^3/hour ;

Scenario 3 – A catastrophic leak from pipeline connection point to ship's storage tank at the marine terminal.

The maximum load velocity of crude oil from tank to ship : 13,000 m^3/hour ;

Diameter of pipe to the ship : 18 inch ;

11.2 Scenario 1 - Phast User Defined Data

Scenario

Release Location

Tank Head 17 m

[Elevation 1 m]

Material

Material

[Material characteristic Flammable only]

[Material to track Mixture]

Discharge parameters

Droplet breakup mechanism

[Droplet break-up mechanism-instantaneous Use flashing correlation]

Dipersion

Dispersion scope

[Specify user-defined averaging time No]

Bund, building and terrain: Default terrain

Dispersing surface

[Surface over which the dispersion occurs Land]

[Surface roughness length User-defined]

[User-defined length 183.156 mm]

Bund, building and terrain

Building definition

[Specify a release building No]

[Building wake effect None]

Flammable

Fireball emissive power

Use vessel burst pressure No

Ignition and explosion

[Supply late igniton location No igniton location]

[Explosion method

TNT]

Explosion prameters

TNT parameters

[Air or ground burst Air burst]

[Default TNT explosion efficiency 0.1 fraction]

Vapour liquid method

[Use of exlosion mass modification factor Early and late explosion]

[Explosion mass modification factor 3]

Pool fire

Parameters

[Radiative fraction for general fires 0.4 fraction]

Radiation levels

[Number of input radiation levels 3]

[Intensity levels (1) 4 kW/m^2]

[Intensity levels (2) 12.5 kW/m^2]

[Intensity levels (3) 37.5 kW/m^2]

DISCHARGE DATA for Weather: Wether folder\Category 1.5/F

Wind Speed: 1.50m/s

Wind Speed at Height (Claculated) 0.46m/s

Pasquill Stability: F

USER-DEFINED QUANTITIES

Material Mixture

Scenario Catastrophic rupture

Inventor 160,625,000. kg

Fixed Duration n/a s

Stagnation data (data at upstream end for long pipe):

-Pressure bar

-Temperature 31.06 degC

-Fluid State Liquid at atmospheric pressure

CALCULATED QUANTITIES

Mass Flow of Air (Vent from Vapor Space only) n/a

Mass Flowrate kg/s

Release Duration n/a s

Orifice or pipe exit data (before atmospheric expansion):

- Pressure n/a bar
- Temperature n/a degC
- Vena contracta Velocity (exit velocity for pipe releases) n/a m/s
- Discharge Coefficent n/a

Final data (after atmosheric expansion):

- Temperature 31.04 degC
- Liquid Mass Fraction 1.00 fraction
- Droplet Diameter 1E++004 um
- Expanded Diameter n/s m
- Velocity 7.04 m/s

DISCHARGE DATA for Weather: Weather folder\Category 1.5/D

Wind Speed: 1.50m/s

Wind Speed at Height (Claculated) 0.96m/s

Pasquill Stability: D

USER-DEFINED QUANTITIES

Material Mixture

Scenario Catastrophic rupture

Inventor 160,625,000. kg

Fixed Duration n/a s

Stagnation data (data at upstream end for long pipe):

-Pressure bar

-Temperature 31.06 degC

-Fluid State Liquid at atmospheric pressure

CALCULATED QUANTITIES

Mass Flow of Air (Vent from Vapor Space only) n/a

Mass Flowrate kg/s

Release Duration n/a s

Orifice or pipe exit data (before atmospheric expansion):

- Pressure n/a bar
- Temperature n/a degC
- Vena contracta Velocity (exit velocity for pipe releases) n/a m/s
- Discharge Coefficent n/a

Final data (after atmosheric expansion):

- Temperature 31.04 degC

- Liquid Mass Fraction 1.00 fraction
- Droplet Diameter 1E++004 um
- Expanded Diameter n/s m
- Velocity 7.04 m/s

DISCHARGE DATA for Weather: Weather folder\Category 5/D

Wind Speed: 5.00 m/s

Wind Speed at Height (Calculated) 3.21 m/s

Pasquill Stability: D

USER-DEFINED QUANTITIES

Material Mixture

Scenario Catastrophic rupture

Inventor 160,625,000. kg

Fixed Duration n/a s

Stagnation data (data at upstream end for long pipe):

-Pressure bar

-Temperature 31.06 degC

-Fluid State Liquid at atmospheric pressure

CALCULATED QUANTITIES

Mass Flow of Air (Vent from Vapor Space only) n/a

Mass Flowrate kg/s

Release Duration n/a s

Orifice or pipe exit data (before atmospheric expansion):

- Pressure n/a bar
- Temperature n/a degC
- Vena contracta Velocity (exit velocity for pipe releases) n/a m/s
- Discharge Coefficent n/a

Final data (after atmosheric expansion):

- Temperature 31.04 degC
- Liquid Mass Fraction 1.00 fraction
- Droplet Diameter 1E++004 um
- Expanded Diameter n/s m
- Velocity 7.04 m/s

11.2.1 Consequence results

Pool Vaporization Results

Pool vaporization segments begin when the cloud has left the pool

		Category 1.5/F	Category 1.5/D	Category 5/D
Liquid Rainout	fraction	0,794149	0,794183	0,794121
Initial Vapor Cloud	kg	2,19489E+07	2,19452E+07	2,19518E+07
Time Pool Left Behind	s	3640,87	3640,87	1419,9

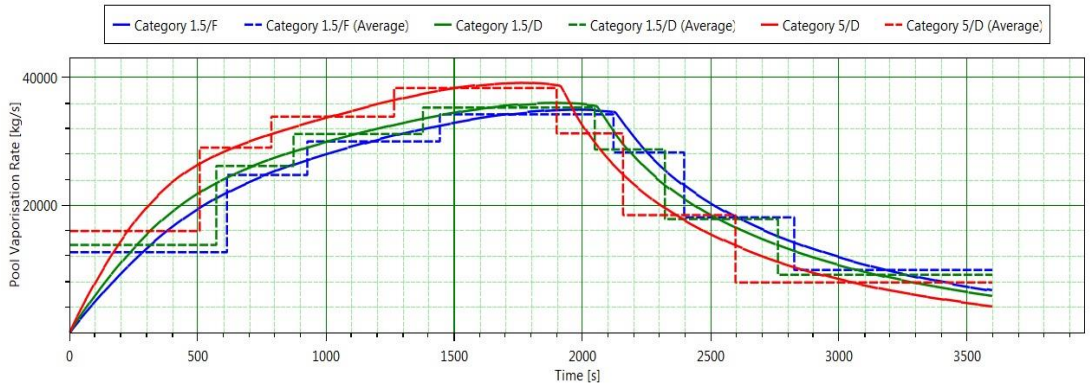


Figure 11.1 : Pool vaporization rate vs time (Scenario 1).

Late Pool Fire Hazard

	Category 1.5/F	Category 1.5/D	Category 5/D
Late Pool Fire Status	Hazard	Hazard	Hazard

Radiation Effects: Late Pool Fire Ellipse

			Distance (m)		
			Category 1.5/F	Category 1.5/D	Category 5/D
Radiation Level	4	Kw/m^2	2412,22	2286,72	2583,73
Radiation Level	12,5	Kw/m^2	1731,77	1613,59	1671,05
Radiation Level	37,5	Kw/m^2	Not Reached	Not Reached	Not Reached

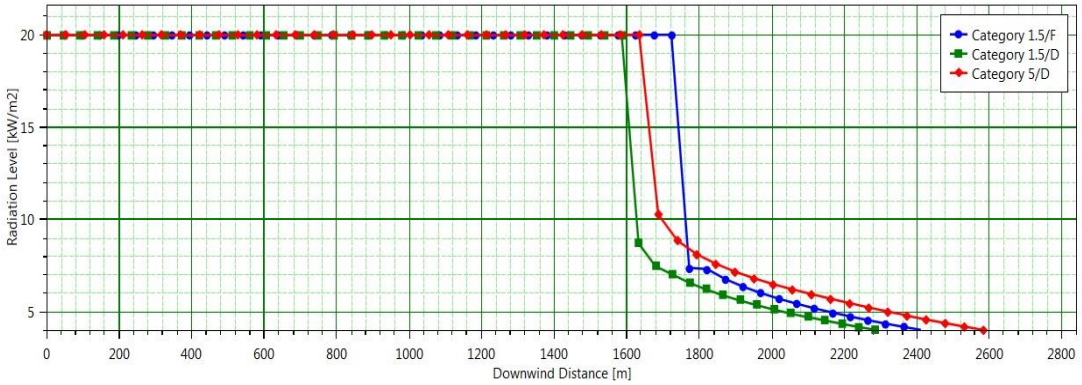


Figure 11.2 : Radiation and distance for late pool fire (Scenario 1).

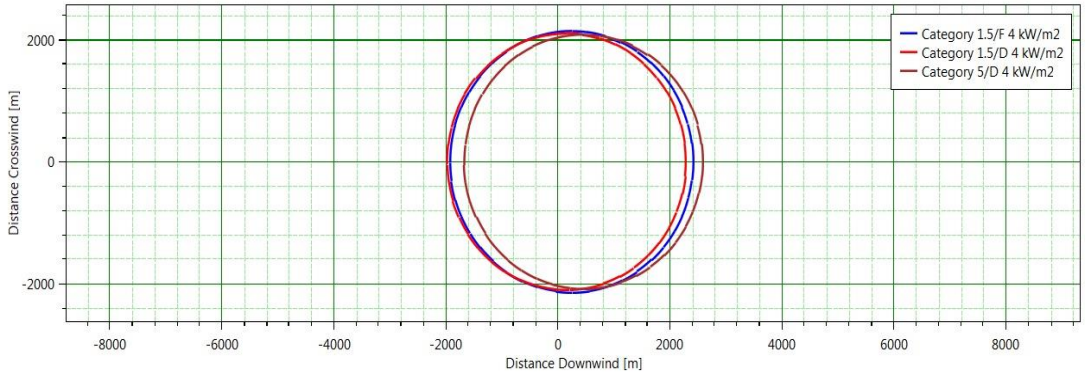


Figure 11.3 : Intensity radii for late pool fire (Scenario 1).

Flash Fire Envelope

			Distance (m) Category		
			Category 1.5/F	1.5/D	Category 5/D
Furthest Extent	3485,9	ppm	14341,7	13679	6803,7
Furthest Extent	6971,8	ppm	11751,6	10985,2	5009,73

			Heights (m) for above distances Category		
			Category 1.5/F	1.5/D	Category 5/D
Furthest Extent	3485,9	ppm	0	0	0
Furthest Extent	6971,8	ppm	0	0	0

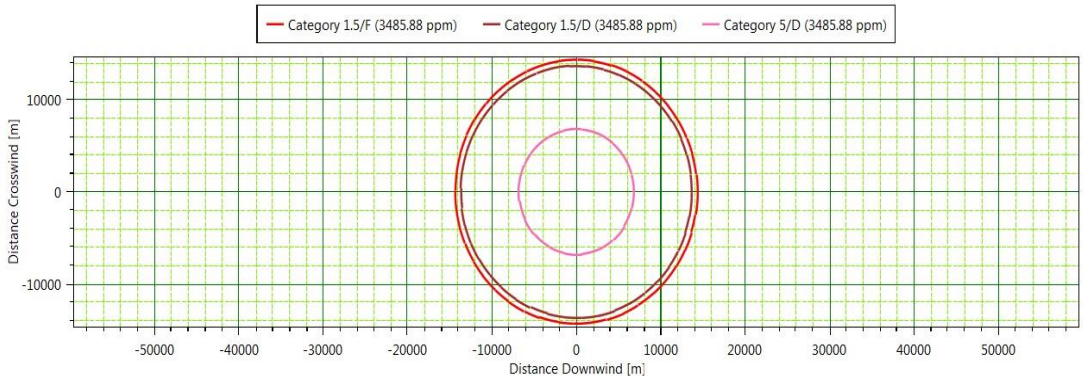


Figure 11.4 : Flash fire envelope (Scenario 1).

11.3 Scenario 2 - Phast User Defined Data

Scenario

Direction

[Outdoor release direction Horizontal]

Hole

Orifice diameter 11.2 mm

Use specified discharge coefficient ? No

Release Location

Tank Head 17 m

[Elevation 1 m]

Material

Material

[Material characteristic Flammable only]

[Material to track Mixture]

Discharge parameters

Droplet breakup mechnism

[Droplet break-up mechanism-instantaneous Use flashing correlation]

[Droplet break-up mechanism-continuous Do not force correlation]

Model seetings

[Atmospheric expansion method Closest initial conditions]

[Is flashing allowed to the orifice ? No flashing in the orifice]

Dipersion

Dispersion scope

[Specify user-defined averaging time No]

Bund, building and terrain: Default terrain

Dispersing surface

[Surface over which the dispersion occurs Land]

[Surface roughness length User-defined]

[User-defined length 183.156 mm]

Bund, building and terrain

Building definition

[Specify a release building No]

[Building wake effect None]

Flammable

Ignition and explosion

[Supply late igniton location No igniton location]

[Explosion methot TNT]

Jet fire method

[Jet fire method Cone model]

Explosion prameters

TNT parameters

[Air or ground burst Air burst]

[Default TNT explosion efficiency 0.1 fraction]

Vapour liquid method

[Use of exlosion mass modification factor Early and late explosion]

[Explosion mass modification factor 3]

Jet fire

Cone model data

[Horizontal options Use standard method]

[Correlation DNV recommend]

Parameters

[Rate modification factor 3]

Radiation levels

[Number of input radiation levels 3]

[Intensity levels (1) 4 kW/m^2]

[Intensity levels (2) 12.5 kW/m^2]

[Intensity levels (3) 37.5 kW/m^2]

Surface emissive power

[Calculation method for surface emissive power Calculate SEP]

Parameters

[Radiative fraction for general fires 0.4 fraction]

Radiation levels

[Number of input radiation levels 3]

[Intensity levels (1) 4 kW/m^2]

[Intensity levels (2) 12.5 kW/m^2]

[Intensity levels (3) 37.5 kW/m^2]

DISCHARGE DATA for Weather**:** Weather folder\Category 1.5/F

Wind Speed:	1.50m/s
Wind Speed at Height (Claculated)	0.46m/s
Pasquill Stability:	F

USER-DEFINED QUANTITIES

Material	Mixture
Scenario	Leak
Inventor	160,625,000. kg
Fixed Duration	n/a s

Stagnation data (data at upstream end for long pipe):

-Pressure	bar
-Temperature	31.06 degC
-Fluid State	Liquid at atmospheric pressure

CALCULATED QUANTITIES

Mass Flow of Air (Vent from Vapor Space only)	n/a
Mass Flowrate	0,894049 kg/s
Release Duration	3,600.00 s

Orifice or pipe exit data (before atmospheric expansion):

- Pressure 1.01 bar

- Temperature 31.03 degC
- Vena contracta Velocity (exit velocity for pipe releases) 20.82 m/s
- Discharge Coefficent 0.60

Final data (after atmosheric expansion):

- Temperature 31.04 degC
- Liquid Mass Fraction 1.00 fraction
- Droplet Diameter 4.7361E+002 um
- Expanded Radius 0.0 m
- Velocity 20.82 m/s
  m/s

DISCHARGE DATA for Weather: Wether folder\Category 1.5/D

Wind Speed: 1.50m/s

Wind Speed at Height (Claculated) 0.96m/s

Pasquill Stability: D

USER-DEFINED QUANTITIES

Material Mixture

Scenario Catastrophic rupture

Inventor 160,625,000. kg

Fixed Duration n/a s

Stagnation data (data at upstream end for long pipe):

-Pressure bar

-Temperature 31.06 degC

-Fluid State Liquid at atmospheric pressure

CALCULATED QUANTITIES

Mass Flow of Air (Vent from Vapor Space only) n/a

Mass Flowrate 0.894049 kg/s

Release Duration 3,600.00 s

Orifice or pipe exit data (before atmospheric expansion):

- Pressure 1.01 bar
- Temperature 31.03 degC
- Vena contracta Velocity (exit velocity for pipe releases) 20.82 m/s
- Discharge Coefficent 0.60

Final data (after atmosheric expansion):

- Temperature 31.04 degC
- Liquid Mass Fraction 1.00 fraction
- Droplet Diameter 4.7361E+002 um
- Expanded Diameter 0.0 m
- Velocity 20.82 m/s

DISCHARGE DATA for Weather: Wether folder\Category 5/D

Wind Speed:	5.00 m/s
Wind Speed at Height (Claculated)	3.21 m/s
Pasquill Stability:	D

USER-DEFINED QUANTITIES

Material	Mixture
Scenario	Catastrophic rupture
Inventor	160,625,000. kg
Fixed Duration	n/a s

Stagnation data (data at upstream end for long pipe):

-Pressure	bar
-Temperature	31.06 degC
-Fluid State	Liquid at atmospheric pressure

CALCULATED QUANTITIES

Mass Flow of Air (Vent from Vapor Space only)		n/a
Mass Flowrate	0.894049	kg/s
Release Duration	3,600.00	s

Orifice or pipe exit data (before atmospheric expansion):

- Pressure	1.01	bar
- Temperature	31.03	degC
- Vena contracta Velocity (exit velocity for pipe releases)	20.82	m/s
- Discharge Coefficent	0.60	

Final data (after atmosheric expansion):

- Temperature	31.03	degC
- Liquid Mass Fraction	1.00	fraction
- Droplet Diameter	4.7261E+002	um
- Expanded Diameter	0.0	m
- Velocity	20.82	m/s

11.3.1 Consequence results

		Category 1.5/F	Category 1.5/D	Category 5/D
Release Segment 1				
Release Duration	s	3600	3600	3600
Liquid Rainout	fraction	0.51299	0.510491	0.488266
Release Segment 1 Cloud Segment 1				
Cloud Segment Duration	s	599.026	534.766	564.063
Pool Vaporization Rate	kg/s	0.240201	0.238444	0.259698
Total Vapor Flowrate	kg/s	0.675611	0.676089	0.717214
Release Segment 1 Cloud Segment 2				
Cloud Segment Duration	s	3000.97	3065.23	3035.94
Pool Vaporization Rate	kg/s	0.448892	0.447655	0.433378
Total Vapor Flowrate	kg/s	0.884302	0.885299	0.890894
Maximum Pool Radius	m	3.71322	3.51409	3.08349

Figure 11.5 : Pool vaporization results (Scenario 2).

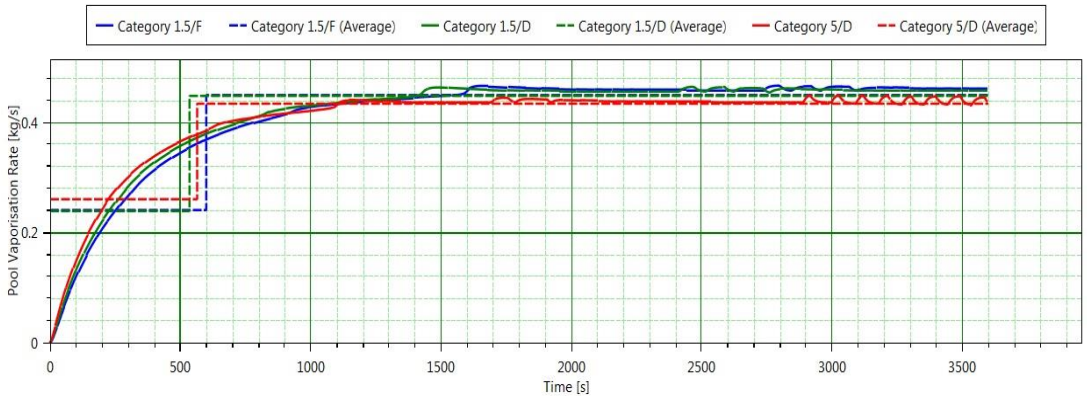


Figure 11.6 : Pool vaporization rate vs time (Scenario 2).

Jet Fire Hazard

Jet fire method used: Cone model – DNV recommended

Jet Fire Status			Category 1.5/F Truncated	Category 1.5/D Truncated	Category 5/D Truncated
Flame Direction			Horizontal	Horizontal	Horizontal
				Distance (m)	
			Category 1.5/F	Category 1.5/D	Category 5/D
Radiation Level	4	kW/m2	25.9629	25.9629	22.8851
Radiation Level	12.5	kW/m2	19.4133	19.4133	16.4428
Radiation Level	37.5	kW/m2	15.5069	15.5069	12.6827

Figure 11.7 : Radiation effects for jet fire ellipse (Scenario 2).

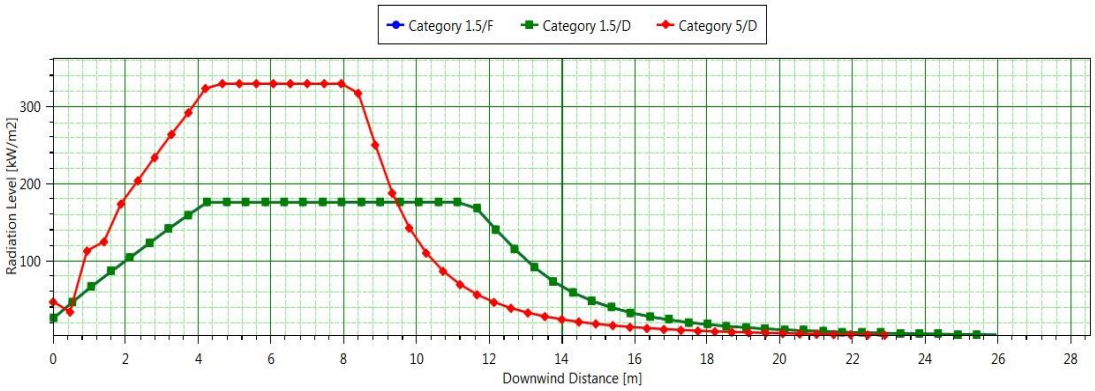


Figure 11.8 : Radiation vs distance for jet fire (Scenario 2).

Early Pool Fire Hazard and Radiation Effects Early Pool Fire Ellipse

Early Pool Fire Status			Category 1.5/F Hazard	Category 1.5/D Hazard	Category 5/D Hazard
			Distance (m)		
			Category 1.5/F	Category 1.5/D	Category 5/D
Radiation Level	4	kW/m2	19.3671	19.4525	20.6934
Radiation Level	12.5	kW/m2	13.4062	13.5032	15.7649
Radiation Level	37.5	kW/m2	7.98925	8.09477	9.30806

Figure 11.9 : Radiation effects for early pool fire ellipse (Scenario 2).

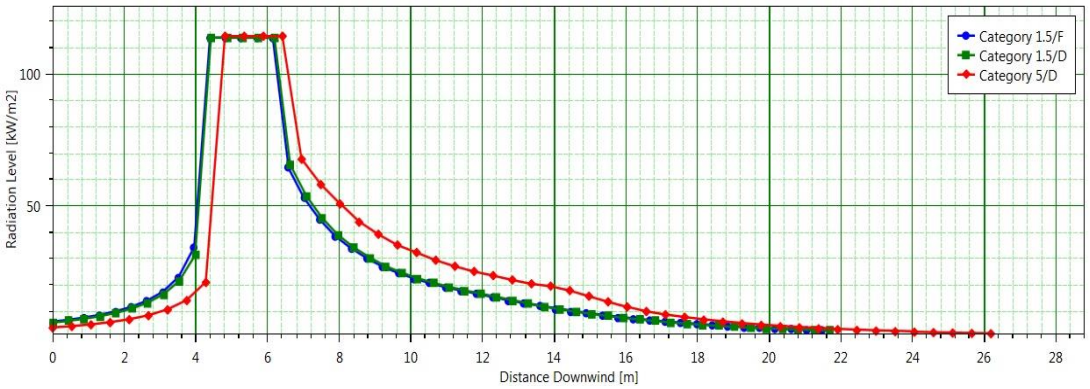


Figure 11.10 : Radiation vs distance for early pool fire (Scenario 2).

Late Pool Fire Hazard and Radiation Effects Late Pool Fire Ellipse

Late Pool Fire Status			Category 1.5/F Hazard	Category 1.5/D Hazard	Category 5/D Hazard
			Distance (m)		
			Category 1.5/F	Category 1.5/D	Category 5/D
Radiation Level	4	kW/m2	36.1381	35.4288	36.8712
Radiation Level	12.5	kW/m2	20.6781	20.5637	25.8571
Radiation Level	37.5	kW/m2	10.0118	10.0718	11.2139

Figure 11.11 : Radiation effects for late pool fire ellipse (Scenario 2).

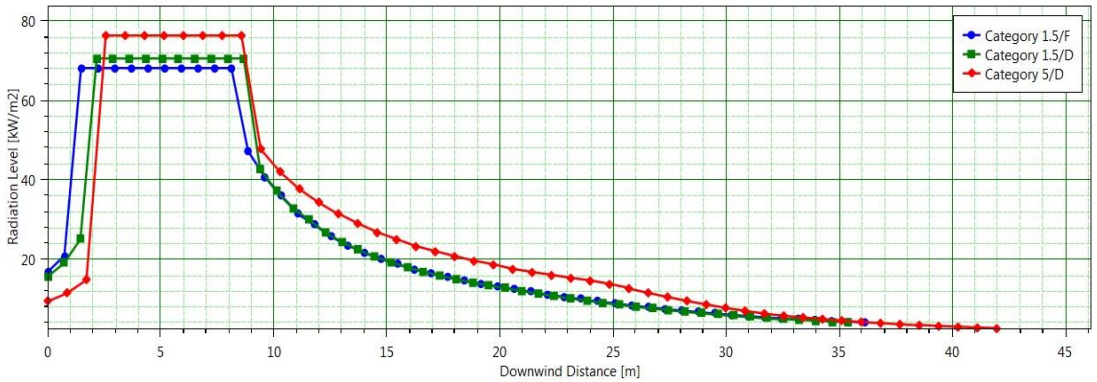


Figure 11.12 : Radiation vs distance for late pool fire (Scenario 2).

Flash Fire Envelope
All flammable results are reported at the cloud centreline height

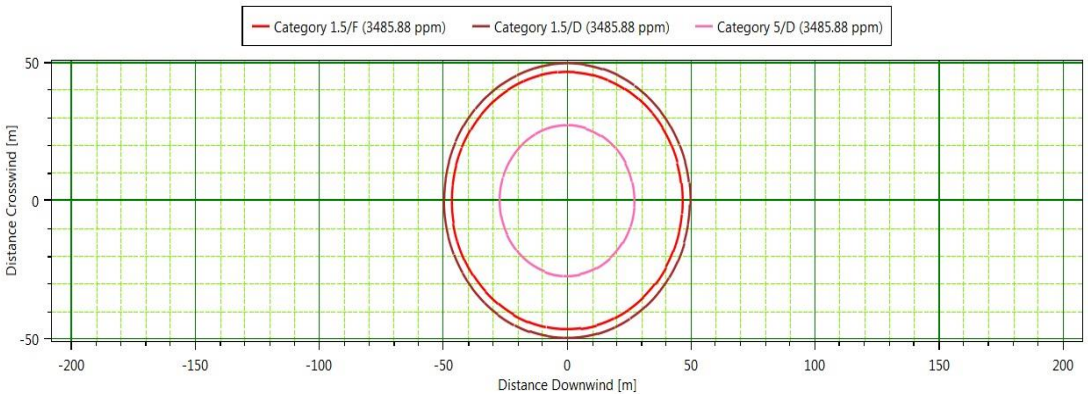


Figure 11.13 : Flash fire envelope (Scenario 2).

11.4 Scenario 3. Phast User Defined Data

Scenario

Release Location

Tank Head 5 m

[Elevation 3 m]

Material

Material

[Material characteristic Flammable only]

[Material to track Mixture]

Discharge parameters

Droplet breakup mechanism

[Droplet break-up mechanism-instantaneous Use flashing correlation]

Dispersion

Dispersion scope

[Specify user-defined averaging time No]

Bund, building and terrain: Default terrain

Dispersing surface

[Surface over which the dispersion occurs Land]

[Surface roughness length User-defined]

[User-defined length 183.156 mm]

Bund, building and terrain: No bund

Bund Properties

[Bund Height 0 m]

[Building area 0 m^2]

[Bund failure modeling Bund cannot fail]

Surface for pools

[Type of surface for pools Concrete]

Bund, building and terrain

Building definition

[Specify a release building No]

[Building wake effect None]

Flammable

Fireball emissive power

Use vessel burst pressure No

Ignition and explosion

[Supply late igniton location No igniton location]

[Explosion methot TNT]

Explosion prameters

TNT parameters

[Air or ground burst Air burst]

[Default TNT explosion efficiency 0.1 fraction]

Vapour liquid method

[Use of exlosion mass modification factor Early and late explosion]

[Explosion mass modification factor 3]

Fireball

Calculation method

[Fireball model DNV recommended]

Parameters

[Mass modification factor 3]

Radiation levels

[Number of input radiation levels 3]

[Intensity levels (1) 4 kW/m^2]

[Intensity levels (2) 12.5 kW/m^2]

[Intensity levels (3) 37.5 kW/m^2]

Pool fire

Parameters

[Radiative fraction for general fires 0.4 fraction]

Radiation levels

[Number of input radiation levels 3]

[Intensity levels (1) 4 kW/m^2]

[Intensity levels (2) 12.5 kW/m^2]

[Intensity levels (3) 37.5 kW/m^2]

DISCHARGE DATA for Weather: Weather folder\Category 1.5/F

Wind Speed: 1.50m/s

Wind Speed at Height (Claculated) 0.81m/s

Pasquill Stability: F

USER-DEFINED QUANTITIES

Material Mixture

Scenario Catastrophic rupture

Inventor 200,000,00. kg

Fixed Duration n/a s

Stagnation data (data at upstream end for long pipe):

-Pressure 19.01 bar

-Temperature 25.00 degC

-Fluid State Non-saturated liquid

CALCULATED QUANTITIES

Mass Flow of Air (Vent from Vapor Space only) n/a

Mass Flowrate kg/s

Release Duration n/a s

Orifice or pipe exit data (before atmospheric expansion):

- Pressure n/a bar
- Temperature n/a degC
- Vena contracta Velocity (exit velocity for pipe releases) n/a m/s
- Discharge Coefficent n/a

Final data (after atmosheric expansion):

- Temperature 24.69 degC
- Liquid Mass Fraction 1.00 fraction
- Droplet Diameter 2.59847E+002 um
- Expanded Radius n/a m
- Velocity 38.79 m/s

DISCHARGE DATA for Weather:	Wether folder\Category 1.5/D	
Wind Speed:		1.50m/s
Wind Speed at Height (Claculated)		1.19m/s
Pasquill Stability:		D
USER-DEFINED QUANTITIES		
Material		Mixture
Scenario		Catastrophic rupture
Inventor		200,000,00. kg
Fixed Duration		n/a s
Stagnation data (data at upstream end for long pipe):		
-Pressure		19.01 bar
-Temperature		25.00 degC
-Fluid State	Non-saturated liquid	
CALCULATED QUANTITIES		
Mass Flow of Air (Vent from Vapor Space only)		n/a
Mass Flowrate		kg/s
Release Duration		n/a s
Orifice or pipe exit data (before atmospheric expansion):		
- Pressure		n/a bar
- Temperature		n/a degC
- Vena contracta Velocity (exit velocity for pipe releases)		n/a m/s
- Discharge Coefficent		n/a
Final data (after atmosheric expansion):		
- Temperature		24.69 degC
- Liquid Mass Fraction		1.00 fraction
- Droplet Diameter		2.59847E+002 um
- Expanded Radius		n/a m
- Velocity		38.79 m/s
DISCHARGE DATA for Weather:	Wether folder\Category 5/D	
Wind Speed:		5.00 m/s
Wind Speed at Height (Claculated)		3.96 m/s
Pasquill Stability:		D
USER-DEFINED QUANTITIES		

Material	Mixture
Scenario	Catastrophic rupture
Inventor	200,000,00. kg
Fixed Duration	n/a s
Stagnation data (data at upstream end for long pipe):	
-Pressure	19.01 bar
-Temperature	25.00 degC
-Fluid State	Non-saturated liquid
CALCULATED QUANTITIES	
Mass Flow of Air (Vent from Vapor Space only)	n/a
Mass Flowrate	kg/s
Release Duration	n/a s
Orifice or pipe exit data (before atmospheric expansion):	
- Pressure	n/a bar
- Temperature	n/a degC
- Vena contracta Velocity (exit velocity for pipe releases)	n/a m/s
- Discharge Coefficent	n/a
Final data (after atmosheric expansion):	
- Temperature	24.69 degC
- Liquid Mass Fraction	1.00 fraction
- Droplet Diameter	2.59847E+002 um
- Expanded Diameter	n/s m
- Velocity	38.79 m/s

11.4.1 Consequence results

Distance to Concentration Results

The height for user defined concentrations is the user defined height 0 m. All toxic results are reported at the toxic effect height 0 m. All flammable results are reported at the cloud centreline height.

Concentration(ppm)	Averaging Time		Distance (m)		
			Category 1.5/F	Category 1.5/D	Category 5/D
UFL (55426.3)	18.75	s	127.998	120.435	184.804
LFL (6971.76)	18.75	s	867.84	875.425	712.008
LFL Frac (3485.88)	18.75	s	1106.28	1107.71	888.01

Concentration(ppm)	Averaging Time		Heights (m) for above distances		
			Category 1.5/F	Category 1.5/D	Category 5/D
UFL (55426.3)	18.75	s	0	0	0
LFL (6971.76)	18.75	s	0	0	0
LFL Frac (3485.88)	18.75	s	0	0	0

Figure 11.14 : Distance to concentration results (Scenario 3).

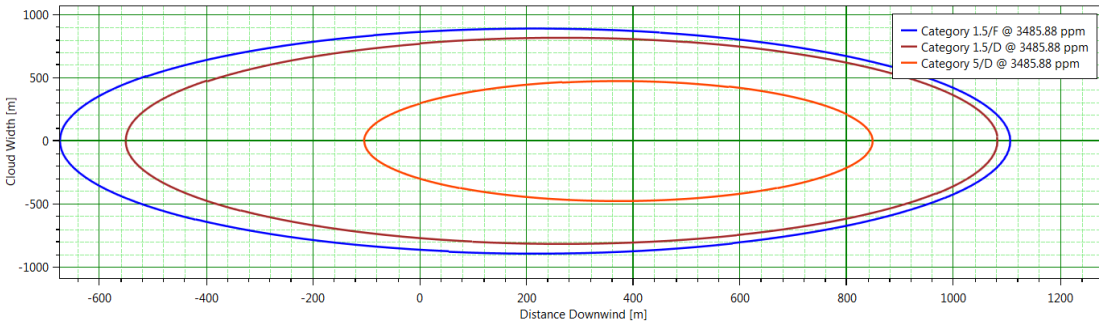


Figure 11.15 : Cloud footprint (Scenario 3).

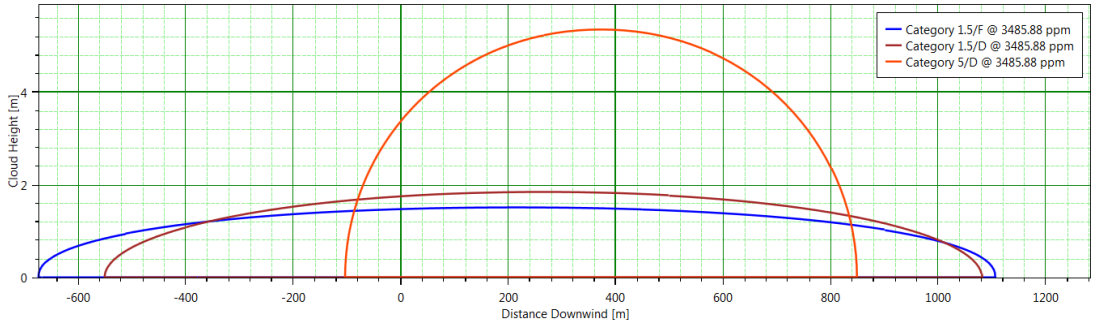


Figure 11.16 : Side view (Scenario 3).

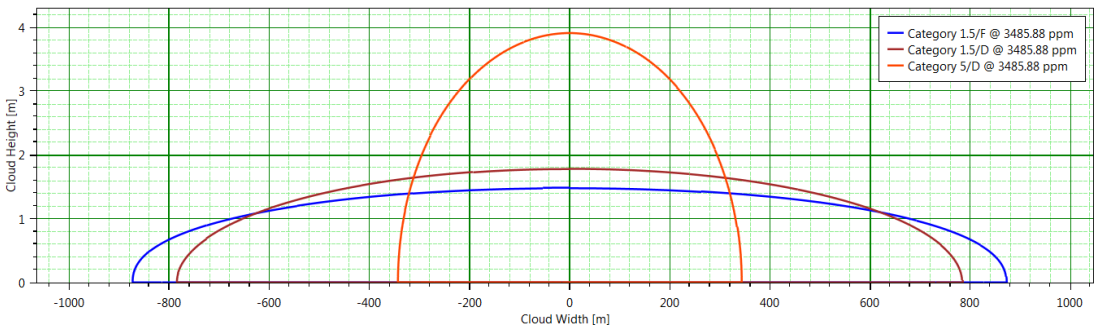


Figure 11.17 : Cross section (Scenario 3).

Flash Fire Envelope

All flammable results are reported at the cloud centreline height.

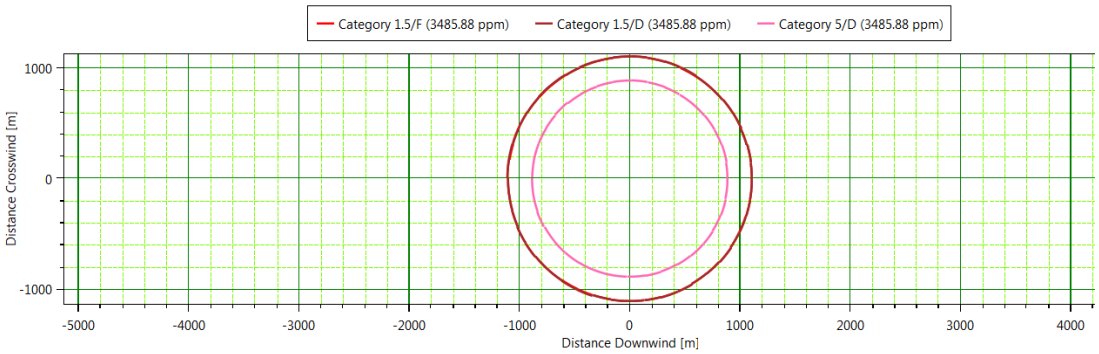


Figure 11.18 : Flash fire envelope (Scenario 3).

12. CONCLUSION

After analyse the scenarios and graphics, manager of plant should follow-up below schedules :

- Prepare Emergency Management Plans
- Provide Training Course to Emergency Team For These Plans
- Make Practices and Minimize Damage, If these accidents will happen
- Determination of Safety Distances
- Damage Assessment

By these ways, effective interventions aimed to possible accidents.

REFERENCES

[1] Lees, F P. (2004) : ‘’Loss Prevention in the Process Industries’’; Butterworth, London 3rd ed.

[2] EC Directive of Major Accident Hazards (1996) : 82/201/EEC 24 June, On the major-accident hazards of certain industrial activities. OJ.L230/1, 5.8.82; also OJ L289/35, 13.10.82 (1982) 96/82/ec ‘Seveso II’ Directive on the control of major accident hazards involving dangerous sustances, official journal of European Communities, L10/13-33.

[3] ‘Integrating Process Safety Mangemnet, Environment, Safety, Helath, and Quality’ (1996): CCPS-Center for Chemical Process of the American Institute of Chemical Engineers, New York.

[4] Skeleton, B. (1997): ‘Process Safety Analysis: an introduction’, Institution of Chemical Engineers.

[5] Cameron, L; Rman, R. (2005): ‘Process Systems Risk Management’, Elsevier Academic Press, NY, ISBN 0-12-156932-2, (pp.474-482,484-,542).

[6] Developing a Risk Management Plan for a Priority Chemical 10 December 2001. Training and Capacity Buildings Programmes in Chemicals and Waste Management United Nations Institute for Training and Reseacrh (UNITAR), Palais des Nations CH-1211 Geneva 10, Switzerland .

[7]http://web.iitd.ac.in/~arunku/files/CEL899_Y13/Industrial%20Risk%20Management_Overview.pdf accesed at 29/03/2015

[8] Marvin Rausand, ‘Preliminary Hazard Lesson Analysis Project’, Department of Production and Quality Engineering Norwegian of Science and Technology, October 7,2005.

[9] Freeman, Raymond A., 1991. ‘Documentation of Hazard and Operability Studies,’ Plant/Operations Progress, July 1991, Vol. 10,No.3.

[10] King, Ralph, 1990. ‘Safety in the Process Industries,’ Butterworth-Heinemann, Ltd.,1990.

[11] U.S. DEPARMENT of Energy, DOE Handbook, DOE-HDBK-1101-2004, ‘Process Safety Management for Highly Hazardous Chemicals,’ Washington, DC, August 2004.

[12] Hendershot, Dennis C., 1992. ‘Documentation and Utilization of the Results Hazard Evaluation Studies,’ prepared for presentation at the AIChE 1992 Spring National Meeting, New Orleans, LA. Rohm and Haas Company, Bristol, PA.

[13] U.S. Department of Energy, DOE Order 5480.19 (Chg2), ‘Conduct of Operations Requirement for DOE Facilities,’ Washington, DC, July 1990.

[14] Title 29 Code of FederalRegulations (CFR) Part 1910, ‘Process Safety Mangement of Highly Hazardous Chemicals; Explosives and Blasting Agents; Final Rule, ‘February 24, 1992.

[15] Fault Tree Handbook U.S. Nuclear Regulatory Commission NUREG-0492, January 1981.

[16] Henley E.J. & Kumamoto H., Probabilistic Risk Assessment; Reliability Engineering, design and Analysis, IEEE Press, New York. 1992.

[17] Manual Fault Tree Analysis code FTA, J.C.H. Schüller, KEMA Nuclear, 40721-NUC-94-4582, 11 January 1995.

[18] R.van der Mark, Generic Fault Trees and the Modeling of Management and Organization, Delft University of Technology, August25, 1996, Delft.

[19] Guidelines for Chemical Process Quantitative Risk Analysis, Center for Chemical Process Safety of the American Institute of Chemical Engineers, 345 East 47th Street, New York, NY 10017 (ISBN 0-8169-0402-2)

[20] Vesely, W.E., et al; Fault Tree Handbook, NUREG-0492; U.S Government Printing Office; January 1981.

[21] Premises for Risk Management, Dutch National Environmental Policy Plan, Ministry of Housing, Physical and Environment, Department for Information and International Relations, P.O. Box 20951, 2500 EZ The Hague, The Netherlands.

[22] AMIR/SPAR, System Engineering Monte-Carlo based advanced software, Malchi Science Sci. Ltd. 1992, P.O. Box 1194, Beer-Sheva, Israel.

[23] Roy Billington, Ronald N.Allan, Pitman, 'Reliability Evaluation of Engineering Systems, Concepts and Techniques', Advanced Publishing Program, Boston, London, Melbourne, 1985.

[24] Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples, Center for chemical process safety of the American Institude of Chemical Engineers, New York, September 1992.

[25] Guidelines for Chemical Process Quantitative Risk Analysis, Center for Chemical process safety of the American Institute of Chemical Engineers, New York, 1989.

[26] Procedures for Conducting Probabilistic Safety Assessment of Nuclear Power Plants (Level I), Safety Series No. 50-P-4, International Atomic Energy Agency, Vienna, 1992, (ISBN 92-0-1023928)

[27] http://www.hrdp-idrm.in/e5783/e17327/e27015/e27739/ 25.03.2015

[28] http://www.interfire.org/termoftheweek.asp?term=1072 24.03.2015.

[29] http://me.queensu.ca/People/Birk/Research/ThermalHazards/bleve/ 24.03.2015

[30]http://response.restoration.noaa.gov/oil-and-chemical-spills/chemical-spills/resources/overpressure-levels-concern.html 24.03.2015

[31] GexCon, Gas Explosion Handbook, Website: http://www.gexcon.com., Accessed on 02/03/2011.

[32] http://www.hrdp-idrm.in/e5783/e17327/e27015/e27768/ 25.03.2015

[33] http://www.hrdp-idrm.in/e5783/e17327/e27015/e27713/ 25.03.2015

[34]http://www.infoplease.com/ipa/A0001451.html 15.04.2015

CURRICULUM VITAE

Name Khalilov	**:** Asadulla KHALILOV
Place of and Date Birth	**:** Guba/Azerbaijan – 13/04/1991
E-Mail	**:** khalilov@itu.edu.tr
Adress	**:** Çeliktepe/Kağıthane Istanbul
EDUCATION	**:** Guba Private Turkish High School
B.Sc.	**:** University of Hacettepe Chemical Engineering
M.Sc.	**:** Istanbul Technical University Chemical Engineering